```
<HTML><HEAD>
<META HTTP-EQUIV="Content-type" CONTENT="text/html; charset=x-sjis">
<!-- <META HTTP-EQUIV="Pragma" CONTENT="no-cache"> -->
<TITLE>Searching PAJ</TITLE>
</HEAD>

<BODY BGCOLOR="#FFFFFF" TEXT="#000000" LINK="#000066" VLINK="#808080"
ALINK="#FF0000" TOPMARGIN="0">
<BR><CENTER><H2><B>PATENT ABSTRACTS OF JAPAN</B></H2></CENTER>

<TABLE BORDER="0" WIDTH="100%">
  <TR><TD WIDTH="40%" VALIGN="top"><BR></TD>
      <TD WIDTH="15%" NOWRAP>(11)Publication number : </TD><TD VALIGN="top"
WIDTH="45%"><B>2002-091827</B></TD></TR>
  <TR><TD WIDTH="40%" VALIGN="top"><BR></TD>
      <TD WIDTH="15%" NOWRAP>(43)Date of publication of application : </TD><TD
VALIGN="top" WIDTH="45%"><B>29.03.2002</B></TD></TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<TABLE BORDER="0" WIDTH="100%">
  <TR>
    <TD VALIGN="top" WIDTH="40%">(51)Int.Cl.</TD>
    <TD VALIGN="top" WIDTH="60%"><PRE><B>   G06F 12/14
</B><BR><B>   G06F 12/00
</B><BR><B>   G06F 17/60
</B><BR></PRE></TD>
  </TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<TABLE BORDER="0" WIDTH="100%">
  <TR>
    <TD WIDTH="15%" NOWRAP VALIGN="top">(21)Application number : </TD><TD
WIDTH="25%" VALIGN="top"><B>2000-284862</B></TD>
    <TD WIDTH="15%" NOWRAP VALIGN="top">(71)Applicant : </TD><TD WIDTH="45%"
VALIGN="top"><B>SANYO ELECTRIC CO LTD<BR></B></TD>
  </TR>
  <TR>
    <TD WIDTH="15%" NOWRAP VALIGN="top">(22)Date of filing : </TD><TD WIDTH="25%"
VALIGN="top"><B>20.09.2000</B></TD>
    <TD WIDTH="15%" NOWRAP VALIGN="top">(72)Inventor : </TD><TD WIDTH="45%"
VALIGN="top"><B>HORI YOSHIHIRO<BR></B></TD>
  </TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

<!--__PRIORITY_DELETE__
<TABLE BORDER="0">
  <TR><TD>(30)Priority</TD></TR>
  <TR>
    <TD VALIGN="top">Priority number : </TD><TD VALIGN="top" NOWRAP><B></B></TD>
    <TD VALIGN="top">    Priority date : </TD><TD
VALIGN="top"><B></B></TD>
    <TD VALIGN="top">    Priority country : </TD><TD
VALIGN="top"><B><NOBR></NOBR></B></TD>
  </TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">
__PRIORITY_DELETE__-->

<TABLE BORDER="0" WIDTH="100%">
```

<TR><TD>(54)<B> DATA TERMINAL EQUIPMENT
</B></TD></TR>
<TR><TD VALIGN="top">

(57)Abstract:
PROBLEM TO BE SOLVED: To provide portable terminal equipment for receiving only required enciphered contents data and/or license key or the like from a distribution server.
SOLUTION: When the receiving request of enciphered contents data {Data}Kc is inputted from a user, a portable telephone set retrieves the recording conditions of a contents ID, license key Kc, reproducing time limit information AC1, reproducing time limit and enciphered contents data {Data}Kc or the like on a loaded memory card. Then, only the enciphered contents data {Data}Kc and license (contents ID, license key Kc, reproducing time limit information AC1 and reproducing time limit), which are not recorded in a license area 1415A and a data area 1415B of the memory card are received from the distribution server.

</TD></TR>
</TABLE>
<HR WIDTH="100%" SIZE="5">

LEGAL STATUS
<TABLE BORDER="0" WIDTH="100%">
<TR><TD WIDTH="50%">[Date of request for examination]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Date of sending the examiner's decision of rejection]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]</TD>
<TD WIDTH="50%" VALIGN="top" ALIGN="left">   </TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Date of final disposal for application]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Patent number]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left">   </TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Date of registration]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Number of appeal against examiner's decision of rejection]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Date of requesting appeal against examiner's decision of rejection]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
<TR><TD WIDTH="50%" VALIGN="top">[Date of extinction of right]</TD>
    <TD WIDTH="50%" VALIGN="top" ALIGN="left"></TD>
</TR>
</TABLE>

<!--__CORRECT_DELETE__
<HR WIDTH="100%" SIZE="5">
CORRECTION
<TABLE BORDER="0">
__CORRECT_DATA__
</TABLE>
__CORRECT_DELETE__-->

<HR>CLAIMS
<HR>[Claim(s)]

[Claim 1]

The license for reproducing the encryption contents data which enciphered contents data, and/or said encryption contents data is received from a distribution server. The data-logging section which is the Data Terminal Equipment which records said encryption contents data and/or said license, and records said encryption contents data and said license,
It has the interface which controls data transfer with the transceiver section which performs the communication link with the exterior, and said data-logging section, the key stroke section for inputting directions, and a control section. Said control section
If the request to receipt of encryption contents data is inputted through said key stroke section
It searches whether the encryption contents data by which request to receipt was carried out are recorded on said data recorder.
And when the existence of the license which can reproduce the encryption contents data by which request to receipt was carried out is searched and said encryption contents data are not recorded on said data-logging section,
And/or, the Data Terminal Equipment which requires distribution of said encryption contents data and/or said license of a distribution server through said transceiver section when said license cannot be found.

[Claim 2]

Said control section is a Data Terminal Equipment according to claim 1 which performs retrieval of said encryption contents data and/or said license after the encryption contents data said transceiver section carries out [data] request to receipt based on the menu information on the encryption contents data received from said distribution server are determined.

[Claim 3]

It is the Data Terminal Equipment according to claim 2 with which said decision of encryption contents data which carries out request to receipt is made by choosing the content ID for specifying the encryption contents data contained in said menu information, and said control section performs retrieval of said encryption contents data and/or said license based on said selected content ID.

[Claim 4]

Said control section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 3 which requires distribution of said encryption contents data of said distribution server through said transceiver section when said encryption contents data are searched and said encryption contents data are not recorded on said data-logging section.

[Claim 5]

Said control section is a Data Terminal Equipment according to claim 4 with which said license is searched when said encryption contents data are recorded on said data recorder.

[Claim 6]

It is the Data Terminal Equipment according to claim 1 which said license consists of the license key for decoding said encryption contents data at least, and the playback limit information that playback of said encryption contents data is restricted, and judges that said license cannot be found when the encryption contents data with which request to receipt of said control section was carried out are recorded on said data-logging section and said license key and said playback limit information are not recorded on said data-logging section.

[Claim 7]

A license key for said license to decode said encryption contents data at least,

It consists of the playback limit information that playback of said encryption contents data is restricted. Said control section
The license key for decoding the encryption contents data by which request to receipt was carried out, and its encryption contents data is recorded on said data-logging section.
The Data Terminal Equipment according to claim 1 judged that said license cannot be found when playback of said encryption contents data is restricted by said playback limit information.

[Claim 8]

Said control section is a Data Terminal Equipment according to claim 7 which transmits the playback limit information after modification inputted from said key stroke section to said distribution server through said transceiver section with said content ID as purchase conditions for said license.

[Claim 9]

It is the Data Terminal Equipment according to claim 3 which acquires said content ID by having a display further by inputting the information for choosing said content ID based on said menu information as which said control section displayed said menu information on said display, and the user was displayed on said display through the key stroke section.

[Claim 10]

Said control section is a Data Terminal Equipment according to claim 9 which said menu information consists of two or more screens including the shift information for shifting to other screens, and will display other screens determined based on said shift information on said display if said shift information is inputted from said input section including the input section for said display to input said shift information.

[Claim 11]

Said control section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 10 which receives said license only when the purchase conditions of said license, and the authentication data and said content ID of said data-logging section acquired through said interface are transmitted to said distribution server through said transceiver section and said authentication data are attested in said distribution server.

[Claim 12]

It has further the data playback section which reproduces said encryption contents data according to said license. Said control section
If the playback demand of encryption contents data is inputted through said key stroke section
Said interface is minded for information required for said data playback section at least, and said encryption contents data from said data-logging section among said licenses over said encryption contents data. A receipt,
A Data Terminal Equipment given in any 1 term of claim 1 to claim 11 which gives the received encryption contents data and said required information to said data playback section.

[Claim 13]

It connects with said bus and has further the authentication data-hold section holding the authentication data to said data-logging section. At the time of playback of encryption contents data said control section
Only when said authentication data are attested in said data-logging section, said interface is minded for information required for said data playback section at least from said data-logging section among said licenses over said encryption contents data. A receipt,
The Data Terminal Equipment according to claim 12 which gives the received encryption contents data and said required information to said data playback section.

[Claim 14]

Said data-logging section is a Data Terminal Equipment given in any 1 term of claim 1 to claim 13 which is a removable data recorder.

<HR>DETAILED DESCRIPTION
<HR>[Detailed Description of the Invention]

[0001]

[Field of the Invention]

This invention relates to the Data Terminal Equipment used in the data distribution system which makes possible the protection of copyrights to the copied information.

[0002]

[Description of the Prior Art]

Each user is able to access network information easily in recent years with the terminal for the individuals [advance / of information communication networks, such as the Internet, etc.] using a portable telephone etc.

[0003]

In such an information communication network, information is transmitted by the digital signal.
It is possible to perform a copy of data, without producing most degradation of the tone quality by such copy, or image quality, even when an individual user copies the music and image data which followed, for example, were transmitted in the above information communication networks.

[0004]

Therefore, if the policy for suitable protection of copyrights is not taken when the creation object with which the access of authors, such as music data and image data, exists on such an information communication network is transmitted, there is a possibility of infringing on a copyright person's access remarkably.

[0005]

On the other hand, top priority is given to the object of protection of copyrights, and supposing it cannot distribute work data through the digital information communication network which carries out sudden expansion size, it will become rather disadvantageous also for the copyright person who can collect a fixed royalty on the occasion of the duplicate of work data fundamentally.

[0006]

Here, about CD (compact disk) which recorded the music data usually sold, if it thinks and sees not taking the case of distribution through the above digital information communication networks but taking the case of the record medium which recorded the digital data, the music copy of data from CD to magneto-optic disks (MD etc.) can be freely performed in principle, as long as the copied music concerned is stopped to an individual activity.
However, the individual user who performs digital sound recording etc. is to pay indirectly the fixed amount of the prices of media, such as the digital sound recorder machine itself and MD, as a deposit to a copyright person.

[0007]

And in view of such information being digital data which do not almost have copy degradation, when the music data which are a digital signal are copied to MD from CD, for protection of copyrights, copying music information to MD of further others as digital data from recordable MD could not do a device constitutionally, and it is come.

[0008]

Since distributing music data and image data to the public through a digital information communication network also from such a situation is an act from which itself receives the limit by a copyright person's public transmission right,

sufficient policy for protection of copyrights needs to be devised.

[0009]

In this case, it is necessary for the contents data received once to prevent being reproduced still more freely about contents data which are the works transmitted to the public through an information communication network, such as music data and image data.

[0010]

Then, the data distribution system by which the distribution server holding the encryption contents data which enciphered contents data distributes encryption contents data through a terminal unit to the memory card with which terminal units, such as a portable telephone, were equipped is proposed.
In this data distribution system, it transmits to a distribution server in the case of the distribution demand of the open cryptographic key and certificate of the memory card beforehand attested by the certificate authority of encryption contents data, and the license key for decoding encryption contents data and encryption contents data to a memory card, after checking having received the certificate with which the distribution server was attested is transmitted.
And in case encryption contents data and a license key are distributed, a distribution server and a memory card generate a different session key for every distribution, by the generated session key, encipher a open cryptographic key and exchange keys a distribution server and between memory cards.

[0011]

Eventually, a distribution server transmits the license which it was enciphered by the open cryptographic key of memory card each, and was further enciphered by the session key, and encryption contents data to a memory card.
And a memory card records the license key and encryption contents data which were received on a memory card.

[0012]

And a cellular phone is equipped with a memory card when reproducing the encryption contents data recorded on the memory card.
A cellular phone also has a specialized circuit for decoding the encryption contents data from a memory card other than the usual telephone function, and reproducing, and outputting to the exterior.

[0013]

Thus, the user of a portable telephone can receive encryption contents data from a distribution server using a portable telephone, and can reproduce the encryption contents data.

[0014]

[Problem(s) to be Solved by the Invention]

However, when receiving encryption contents data from a distribution server, a portable telephone receives the purchase conditions which set up the count of playback of the license key which decodes encryption contents data with encryption contents data, and encryption contents data, playback length, etc. from a distribution server, and records them on a memory card.

[0015]

Moreover, a portable telephone reproduces encryption contents data, when not restricted by a count of playback, playback length, etc. which playback of encryption contents data received when reproducing encryption contents data.

[0016]

Furthermore, a portable telephone may receive only encryption contents data from other than a distribution server, and may record them on a memory card.

[0017]

Therefore, although encryption contents data are recorded on the memory card, when

the license key is not recorded on a memory card, encryption contents data and a license key are recorded on the memory card, but when playback of encryption contents data is restricted by the count of playback, playback length, etc., the case where encryption contents data and a license key are not recorded on a memory card etc. is assumed.

[0018]

having required distribution of encryption contents data, a license key, etc. of the distribution server promptly, when the distribution demand of encryption contents data was carried out from a user in this case -- if -- the same encryption contents data and a license key are received from a distribution server -- ******** -- the same encryption contents data -- receiving -- a tariff -- multiple-times payment -- it may be unacquainted and a problem arises.

[0019]

Moreover, in order to receive encryption contents data from a distribution server, there is also a problem of needing unnecessary time amount.

[0020]

Then, it is made in order that this invention may solve this problem, and the object is offering the Data Terminal Equipment which receives chisels, such as required encryption contents data and/or a license key, from a distribution server.

[0021]

[The means for solving a technical problem and an effect of the invention]

The Data Terminal Equipment by this invention receives the license for reproducing the encryption contents data and/or encryption contents data which enciphered contents data from a distribution server.
The data-logging section which is the Data Terminal Equipment which records encryption contents data and/or a license, and records encryption contents data and a license,
It has the interface which controls data transfer with the transceiver section which performs the communication link with the exterior, and the data-logging section, the key stroke section for inputting directions, and a control section. A control section
If the request to receipt of encryption contents data is inputted through the key stroke section
It searches whether the encryption contents data by which request to receipt was carried out are recorded on the data-logging section.
And when the existence of the license for reproducing the encryption contents data by which request to receipt was carried out is searched and encryption contents data are not recorded on the data-logging section,
And/or, when there is no license, distribution of encryption contents data and/or a license is required of a distribution server through the transceiver section.

[0022]

In the Data Terminal Equipment by this invention, if the request to receipt of encryption contents data is inputted through the key stroke section from a user, a control section will search whether the encryption contents data and/or the license with which request to receipt was made are recorded on the data-logging section, and will require distribution of the encryption contents data which are not recorded on the data-logging section, and/or a license of a distribution server.
That is, a Data Terminal Equipment receives only required encryption contents data and a required license from a distribution server according to the encryption contents data in the data-logging section, and the record situation of a license, and records them on the data-logging section.

[0023]

Therefore, according to this invention, the encryption contents data in the data-logging section and the duplicate record of a license can be prevented.

[0024]

Moreover, according to this invention, it can prevent paying the useless tariff by overlapping and receiving a license to a distribution server.

[0025]

Furthermore, according to this invention, it can prevent that useless time amount generates encryption contents data by overlapping and receiving.

[0026]

Preferably, the control section of a Data Terminal Equipment performs retrieval of encryption contents data and/or a license, after the encryption contents data the transceiver section carries out [data] request to receipt based on the menu information on the encryption contents data received from the distribution server are determined.

[0027]

A Data Terminal Equipment performs retrieval of encryption contents data and/or a license, after the encryption contents data which carry out request to receipt are determined based on the menu information received from the distribution server.

[0028]

Therefore, according to this invention, it can judge to accuracy whether the encryption contents data and the license by which request to receipt was carried out are recorded on the data-logging section.

[0029]

The decision of encryption contents data which carries out request to receipt is preferably made by choosing the content ID for specifying the encryption contents data contained in menu information, and a control section performs retrieval of encryption contents data and/or a license based on the selected content ID.

[0030]

A user chooses the encryption contents data which carry out request to receipt by specifying the content ID of encryption contents data.
If it does so, the control section of a Data Terminal Equipment will extract the content ID of selected encryption contents data, and will search whether encryption contents data and/or a license are recorded on the data-logging section based on the extracted content ID.

[0031]

Therefore, according to this invention, retrieval of the encryption contents data in the data-logging section and/or a license can be performed to accuracy.

[0032]

Preferably, the control section of a Data Terminal Equipment requires distribution of encryption contents data of a distribution server through the transceiver section, when encryption contents data are searched and encryption contents data are not recorded on the data-logging section.

[0033]

The control section of a Data Terminal Equipment requires distribution of encryption contents data and a license of **** which searches the license in the data-logging section to a distribution server, when the encryption contents data in the data-logging section are searched using content ID and encryption contents data are not recorded on the data-logging section.

[0034]

Therefore, according to this invention, the encryption contents data in the data-logging section and the record situation of a license are searched promptly, and required encryption contents data and a required license can be received from a distribution server according to that record situation.

[0035]

Preferably, the control section of a Data Terminal Equipment searches a license,

when encryption contents data are recorded on the data-logging section.

[0036]

The control section of a Data Terminal Equipment searches a license, after checking that encryption contents data are not recorded on the data-logging section.

[0037]

Therefore, according to this invention, by performing only required retrieval, retrieval time can be shortened and exact retrieval can be performed.

[0038]

Preferably, a license consists of the license key for decoding encryption contents data at least, and the playback limit information that playback of encryption contents data is restricted, and the encryption contents data by which request to receipt was carried out are recorded on the data recorder, and a control section judges that there is no license, when a license key and playback limit information are not recorded on the data-logging section.

[0039]

When the license key and playback limit information which constitute a license are not recorded on the data-logging section, the control section of a Data Terminal Equipment judges that the license of encryption contents data by which request to receipt was carried out wants to exist.

[0040]

Therefore, according to this invention, when only encryption contents data are recorded on the data-logging section, a license key and playback limit information can be received from a distribution server.

[0041]

A license consists preferably of the license key for decoding encryption contents data at least, and the playback limit information restrict playback of encryption contents data, and it judges that there is [control section] nothing in a license when the license key for decoding the encryption contents data by which request to receipt was carried out, and its encryption contents data is recorded on the data-logging section and playback of encryption contents data is restricted by playback limit information.

[0042]

When only the playback limit information which constitutes a license is not recorded on the data-logging section, the control section of a Data Terminal Equipment judges that the license of encryption contents data by which request to receipt was carried out does not exist.

[0043]

Therefore, according to this invention, when only playback limit information is not recorded on the data-logging section, playback limit information can be received from a distribution server, and a license can be acquired.

[0044]

Preferably, the control section of a Data Terminal Equipment transmits to a distribution server through the transceiver section with content ID as purchase conditions for a license of the playback limit information after modification inputted from the key stroke section.

[0045]

The control section of a Data Terminal Equipment will transmit the purchase conditions set up with content ID to a distribution server, if the purchase conditions of encryption contents data are set up by changing only playback limit information.
And a Data Terminal Equipment receives playback limit information from a distribution server, and records it on the data-logging section.

[0046]

Therefore, according to this invention, also when a license is purchased, encryption contents data are reproduced and a license is lost, encryption contents data can be reproduced by newly purchasing only playback limit information from a distribution server.

[0047]

Preferably, content ID is acquired by equipping a Data Terminal Equipment with a display further, and inputting the information for choosing content ID based on the menu information as which the control section displayed menu information on the display, and the user was displayed on the display through the key stroke section.

[0048]

The menu information distributed from the distribution server is displayed on the display of a Data Terminal Equipment.
And a user inputs the information for choosing the content ID of encryption contents data which looks at the menu information displayed on the display, and wishes to receive from the key stroke section.
If it does so, a control section will acquire the content ID chosen through the key stroke section.

[0049]

Therefore, according to this invention, a user can determine the encryption contents data which wish to receive based on vision information.
Moreover, since the information for choosing content ID is inputted according to this invention, a control section can perform retrieval of encryption contents data and/or a license promptly based on the selected content ID.

[0050]

Preferably, menu information consists of two or more screens including the shift information for shifting to other screens, and a control section will display other screens determined based on shift information on a display, if shift information is inputted from the input section including the input section for a display to input shift information.

[0051]

If a user inputs and does shift information so when the encryption contents data which wish to receive are not contained in the menu information displayed on the display of a Data Terminal Equipment, the control section of a Data Terminal Equipment will shift to the next screen, and will display new menu information on a display.

[0052]

Therefore, according to this invention, the encryption contents data which wish to receive can be chosen from many encryption contents data.

[0053]

Preferably, the control section of a Data Terminal Equipment receives a license, only when the purchase conditions of a license, and the authentication data and content ID of the data-logging section which were acquired through the interface are transmitted to a distribution server through the transceiver section and authentication data are attested in a distribution server.

[0054]

Only when a distribution server attests the authentication data sent from the data-logging section, a Data Terminal Equipment receives a license.

[0055]

Therefore, according to this invention, it can license only to the regular data-logging section.
Consequently, protection of encryption contents data can be aimed at.

[0056]

A Data Terminal Equipment is preferably equipped further with the data playback section which reproduces encryption contents data according to a license, and a control section will give a receipt, its received encryption contents data, and required information through an interface to the data playback section from the data-logging section among the licenses over encryption contents data for information required for the data playback section at least, and encryption contents data, if the playback demand of encryption contents data is inputted through the key-stroke section.

[0057]

A control section gives drawing, encryption contents data, and information required for playback to the data playback section from the data-logging section only for information required for playback among the various information which constitutes a license at the time of playback of encryption contents data.
And the data playback section decodes and reproduces encryption contents data using required information.

[0058]

Therefore, according to this invention, information required for playback can restrict playback of encryption contents data.

[0059]

Preferably, a Data Terminal Equipment is further equipped with the authentication data-hold section holding the authentication data to the data-logging section, and at the time of playback of encryption contents data, a control section gives [among the licenses over encryption contents data] a receipt and its received encryption contents data to the data playback section through an interface from the data-logging section for information required for the data playback section at least, only when authentication data are attested in the data-logging section.

[0060]

Only when reproducing the encryption contents data received from the distribution server and the justification of a Data Terminal Equipment to the data-logging section is checked, a Data Terminal Equipment reproduces a receipt and encryption contents data for encryption contents data from the data-logging section.

[0061]

Therefore, according to this invention, only a regular Data Terminal Equipment can reproduce encryption contents data.
Consequently, the illegal copy of encryption contents data etc. can be prevented and protection can be aimed at.

[0062]

It is a data recorder with the data-logging section it is desirable and removable from a Data Terminal Equipment.

[0063]

a Data Terminal Equipment will boil and record the encryption contents data and license which were received on a removable data recorder, if encryption contents data and a license are received from a distribution server.

[0064]

Therefore, according to this invention, encryption contents data and/or a license are recordable on two or more data recorders.

[0065]

[Embodiment of the Invention]

It explains to a detail, referring to a drawing about the gestalt of operation of this invention.
In addition, the same sign is given to the same or a considerable part among drawing, and the explanation is not repeated.

[0066]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">Drawing 1</A>
is a schematic diagram for explaining notionally the whole data distribution system configuration which distributes the encryption contents data which the personal digital assistant equipment by this invention makes a reproductive object to a memory card.

[0067]

In addition, although explained taking the case of the data distribution structure of a system which distributes digital music data to each cellular-phone user through a portable telephone network below, this invention can be applied, without being limited in such a case, when distributing the contents data as other works, for example, image data, dynamic-image data, etc., so that it may become clear by the following explanation.

[0068]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
, the distribution carrier 20 relays the distribution demand (distribution request) from each cellular-phone user who got through the cellular-phone network of self to a license server.
The license server 10 which manages the music data with which copyright exists [whether the memory card 110 with which a cellular-phone user's portable telephone 100 accessed in quest of data distribution was equipped has just authentication data, and]
Namely, after performing authentication processing of whether to be the memory card of normal and enciphering music data (it is also called contents data below) with a predetermined cipher system to a just memory card
It licenses as information required for the cellular phone company which is the distribution carrier 20 for distributing data in order to reproduce such encryption contents data and encryption contents data.

[0069]

The distribution carrier 20 distributes encryption contents data and a license through a cellular-phone network and a portable telephone 100 to the memory card 110 with which the portable telephone 100 which transmitted the distribution demand through the cellular-phone network of self was equipped.

[0070]

In
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
, it has the composition that a cellular-phone user's portable telephone 100 is equipped with the removable memory card 110, for example.
A memory card 110 is given to the music playback section in a portable telephone 100 (not shown) after decoding the encryption performed in a receipt and the above-mentioned distribution in the encryption contents data received by the portable telephone 100.

[0071]

furthermore -- for example, the head telephone 130 grade which the cellular-phone user connected to the portable telephone 100 -- minding -- such contents data --

"-- reproducing, " carrying out and hearing is possible.

[0072]

Below, it will combine with such a license server 10 and the distribution carrier 20, and will be named the distribution server 30 generically.

[0073]

Moreover, suppose that the processing which transmits contents data to each portable telephone etc. is called "distribution" from such a distribution server 30.

[0074]

It becomes a difficult configuration to play music in response to distribution of contents data first, by considering as such a configuration, from the distribution server 30, if a memory card 110 is not used.

[0075]

And in the distribution carrier 20, it becomes easy that the distribution carrier 20 collects the royalty generated by carrying out counting of the frequency whenever it distributes the contents data for one music whenever a cellular-phone user receives contents data (download) with the phonecall charges of a portable telephone, then for a copyright person to secure a royalty.

[0076]

Being needed on a system, in order to make refreshable the contents data enciphered and distributed in a configuration as shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
at the user side of a cellular phone
It is a method for distributing the cryptographic key in a communication link to the 1st. Further to the 2nd
It is the method itself which enciphers contents data to distribute, and is the configuration of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.

[0077]

The recording apparatus and data playback terminal (the data playback terminal which can reproduce contents is also called portable telephone.) with which authentication and the check function of this invention of operation of as opposed to [in / especially in a gestalt / the time of distribution and generating of each reproductive session] the migration place of these contents data were enriched, and un-attesting or a decode key was torn
the following -- being the same -- by preventing the output of the contents data to receive explains the configuration which strengthens the protection of copyrights of contents data.

[0078]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000004"
TARGET="tjitemdrw">Drawing 2</A>
is drawing explaining properties, such as data for the communication link used, and information, in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
.

[0079]

First, the data distributed from the distribution server 30 are explained.
Data(s) are contents data, such as music data.
Encryption which can be decoded with the license key Kc is given to the contents data Data.
Encryption contents {data Data} Kc to which encryption which can be decoded with the license key Kc was given is distributed to a cellular-phone user from the distribution server 30 in this format.

[0080]

In addition, in the following, it shall be shown that a notation called {Y} X gave encryption which can be decoded with the decode key X for Data Y.

[0081]

Furthermore, from the distribution server 30, additional information Data-inf as plaintext information, such as copyright about contents data or server access relation, is distributed with encryption contents data.
Moreover, the transaction ID which is Control Code for specifying distribution of the encryption contents data from the distribution server 30, a license key, etc. is exchanged between the distribution server 30 and a portable telephone 100.
Furthermore, the license ID which is Control Code which can specify issuance of the content ID which is a code for identifying the contents data Data as license information, and a license
Are generated based on the license purchase conditions AC including information determined by assignment from a user side, such as the number of licenses, and functional definition.
The playback length AC2 grade which are the access-restriction information AC 1 which is the information about the limit to access of a recording device (memory card), and the control information in a data playback terminal exists.
Henceforth, suppose that the license key Kc, content ID, License ID, the count length AC 1 of playback, and the playback length AC 2 are combined, and it is named a license generically.

[0082]

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000005" TARGET="tjitemdrw">Drawing 3</A>
is drawing explaining properties, such as data for employment of the authentication used in the data distribution system shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003" TARGET="tjitemdrw">drawing 1</A>
, and an inhibited class list, and information.

[0083]

In the gestalt of operation of this invention, for every class of the portable telephone which reproduces a recording apparatus (memory card) and contents data, the inhibited class list CRL (Class Revocation List) is employed so that distribution of contents data and playback can be forbidden.
Below, Notation CRL may express the data in an inhibited class list if needed.

[0084]

The inhibited class list data CRL which listed the class of the portable telephone with which distribution of a license and playback are forbidden, and a memory card are contained in inhibited class list related information.

[0085]

While the inhibited class list data CRL are managed within the distribution server

30, record maintenance of them is carried out also into a memory card.
Although it is necessary to upgrade at any time and to update data, about modification of data, such an inhibited class list judges the existence of renewal of the inhibited class list received from the portable telephone on the basis of the time at the time of distributing the license of encryption contents data, a license key, etc. fundamentally, and when not updated, it distributes the updated inhibited class list to a portable telephone.
moreover, the difference which reflected only the changed part about modification of an inhibited class list -- ** considered as the configuration which generates data CRL_dat from the distribution server 30 side, and by which the inhibited class list CRL of [in a memory card] is rewritten according to this is possible.
Moreover, about the version of an inhibited class list, CRL_ver is outputted from a memory card side and version control is performed by checking this by the distribution server 30 side.
difference -- the information on a new version is also included in data CRL_dat.

[0086]

Thus, supply of the license key to the portable telephone and memory card by which the decode key of a proper was torn is forbidden to the class of a class proper, i.e., a portable telephone, and memory card by carrying out maintenance employment of the inhibited class list CRL not only a distribution server but into a memory card.
It becomes impossible for this reason, for playback of contents data to move contents data in a portable telephone at a memory card.

[0087]

Thus, the inhibited class list CRL of [in a memory card] is considered as the configuration which updates data serially at the time of distribution.
Moreover, management of the inhibited class list CRL of [in a memory card] is considered as the configuration which can alter the inhibited class list data CRL from an upper level neither with a file system nor an application program by recording on a tamper REJISUTANTO module (Tamper Resistance Module) within a memory card independently of an upper level etc.
Consequently, the protection of copyrights about data can be made firmer.

[0088]

The open cryptographic keys KPpn and KPmci of a proper are formed in a portable telephone and a memory card, respectively, and the open cryptographic keys KPpn and KPmci can be decoded to a portable telephone, respectively with the secrecy decode key Kpn of a proper, and the secrecy decode key Kmci of a memory card proper.
These disclosure cryptographic key and a secrecy decode key have a different value for every class of every class of portable telephone, and memory card.
These open cryptographic keys and a secrecy decode key are named generically, and a class key is called.

[0089]

Moreover, Crtfn and Cmci are prepared, respectively as a data playback terminal (portable telephone) and a class certificate of a memory card.
These class certificates have different information for every class of a memory card and a contents playback terminal.
To the class key with which the code with a class key was broken, namely, the secrecy decode key was acquired, it is listed by the inhibited class list and set as the prohibition object of license issuance.

[0090]

The open cryptographic key and class certificate of these memory cards and a contents playback terminal proper are recorded [the authentication data {KPmci//Cmci} KPma and in the form of {KPpn//Crtfn} KPma] on a memory card and a data playback terminal (portable telephone), respectively at the time of shipment.
Although the back is explained to a detail, KPma is a open authentication key common to the whole distribution system.

[0091]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000006"
TARGET="tjitemdrw">Drawing 4</A>
is drawing which summarizes the property of the key in connection with encryption, and is explained in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
.

[0092]

As a cryptographic key for the nondisclosure in the data transfer between the outside of a memory card, and a memory card, whenever distribution of contents data and playback are performed, the common keys Ks1-Ks3 generated in the distribution server 30, a portable telephone 100, and a memory card 110 are used.

[0093]

here, the common keys Ks1-Ks3 are the unit of the communication link between a distribution server, a portable telephone, or a memory card, or the unit of access -- "-- it is the common key of a proper generated in every session", and suppose that these common keys Ks1-Ks3 are also called a "session key" to below.

[0094]

These session keys Ks1-Ks3 are managed by a distribution server, a portable telephone, and the memory card by having the value of a proper for every communication link session.
Specifically, the session key Ks1 is generated for every distribution session by the distribution server.
The session key Ks2 is generated for every distribution session and playback session by the memory card, and the session key Ks3 is generated for every playback session in a portable telephone.
In each session, the security reinforcement in a session can be raised by delivering and receiving these session keys, and transmitting a license key etc. in response to the session key generated by other devices, after performing encryption by this session key.

[0095]

Moreover, the secrecy decode key Km of a proper exists for every memory card which can decode the data enciphered as a key for managing data processing in a memory card 110 by open cryptographic key KPm which is called a memory card, and which is set up for every medium, and the open cryptographic key KPm.

[0096]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000007"
TARGET="tjitemdrw">Drawing 5</A>
is the outline block diagram showing the configuration of a license server 10 shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
.

[0097]

The information database 304 for a license server 10 to hold the data which enciphered contents data according to the predetermined method, and delivery information, such as License ID,
The accounting database 302 for holding the accounting information which followed the access initiation to contents data for every cellular-phone user,
The CRL database 306 which manages the inhibited class list CRL, and the menu database 307 holding the menu of the contents data held at the information database,
The distribution record database 308 holding the transaction ID which specifies distribution of contents data, a license key, etc.,
A bus BS 1 is minded for the data from the information database 304, the accounting database 302, the CRL database 306, the menu database 307, and the distribution record database 308. A receipt,
It has the data-processing section 310 for performing predetermined processing, and the communication device 350 for performing data transfer between the distribution carrier 20 and the data-processing section 310 through a communication network.

[0098]

The distribution control section 315 for the data-processing section 310 to control actuation of the data-processing section 310 according to the data on a bus BS 1,
The session key generating section 316 for being controlled by the distribution control section 315 and generating the session key Ks1 at the time of a distribution session,
The authentication key attaching part 313 holding the open authentication key for decoding the authentication data KPma for the authentication sent from the memory card and the portable telephone {KPmci//Cmci},
The authentication data KPma for the authentication sent from the memory card and the portable telephone {KPmci//Cmci} are received through a communication device 350 and a bus BS 1.
The decode processing section 312 which performs decode processing with the open authentication key KPma from the authentication key attaching part 313,
The session key Ks1 generated from the session key generating section 316 is enciphered using the open cryptographic key KPmci obtained by the decode processing section 312.
The encryption processing section 318 for outputting to a bus BS 1 and the decode processing section 320 which performs decode processing in response to the data transmitted after being enciphered by the session key Ks1 from a bus BS 1 are included.

[0099]

The data-processing section 310 contains the encryption processing section 326 for enciphering further the license key Kc and the playback length AC 2 which are given from the distribution control section 315 by the open cryptographic key KPm of the memory card proper obtained by the decode processing section 320, and the encryption processing section 328 for enciphering further and outputting the output of the encryption processing section 326 to a bus BS 1 by the session key Ks2 to which it is given from the decode processing section 320.

[0100]

About the actuation in the distribution session of a license server 10, the back is explained to a detail using a flow chart.

[0101]

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000008" TARGET="tjitemdrw">Drawing 6</A>
is an outline block diagram for explaining the configuration of the portable telephone 100 shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"

TARGET="tjitemdrw">drawing 1</A>

.

[0102]

A portable telephone 100 contains the controller 1106 for controlling actuation of a portable telephone 100 through the bus BS 2 and Bus BS 2 for performing data transfer of the transceiver section 1104 for changing into baseband signaling in response to the signal from the antenna 1102 for receiving the signal by which a radio transmission is carried out with a cellular-phone network, and an antenna 1102, or modulating the data from a portable telephone, and giving an antenna 1102, and each part of a portable telephone 100.

[0103]

A portable telephone 100 contains the voice playback section 1112 for reproducing voice further based on the received data given through a database BS 2 in the display 1110 and the usual call actuation for giving a cellular-phone user the information outputted from the key stroke section 1108 and the controller 1106 grade for giving the directions from the outside to a portable telephone 100 as vision information.

[0104]

A portable telephone 100 contains the terminal 1114 for outputting further the output of DA converter 1113 which changes the output of the voice playback section 1112 into an analog signal from a digital signal, and DA converter 1113 to an external output unit etc.

[0105]

A portable telephone 100 contains the microphone 1115 which inputs the sound signal about which the user of a portable telephone 100 spoke, A-D converter 1116 which changes the sound signal from a microphone 1115 into a digital signal from an analog signal, and the voice coding section 1117 which encodes according to a predetermined method and gives the digital signal from A-D converter 1116 to a bus BS 2 in the further usual call actuation.

[0106]

A portable telephone 100 includes the memory interface 1200 for controlling transfer of the data between the removable memory cards 110, the memory cards 110, and Buses BS 2 for memorizing the contents data (music data) from the distribution server 30, and carrying out decryption processing further.

[0107]

a portable telephone -- 100 -- further -- a portable telephone -- a class (class) -- every -- respectively -- setting up -- having -- disclosure -- a cryptographic key -- KPp -- one -- and -- a class -- a certificate -- Crtf -- one -- disclosure -- decode -- a key -- KPma -- decoding -- things -- the -- justification -- it can attest -- a condition -- having enciphered -- authentication -- data -- {-- KPp -- one -- /-- /-- Crtf -- one --} -- KPma -- holding -- authentication -- data-hold -- the section -- 1202 -- containing .
Here, the class n of a portable telephone (Data Terminal Equipment) 100 presupposes that it is n= 1.

[0108]

A portable telephone 100 contains Kp1 attaching part 1204 which holds further Kp1 which is the decode key of a portable telephone (contents regenerative circuit) proper, and the decode processing section 1206 which obtains the session key Ks2 which decoded carrier beam data by Kp1 from the bus BS 2, and was generated by the memory card 110.

[0109]

A portable telephone 100 further
The session key generating section 1210 which generates the session key Ks3 for enciphering the data which set and are carried out on a bus BS 2 between memory cards 110 in the playback session which reproduces the contents data memorized by

the memory card 110 with a random number etc.,
The encryption processing section 1208 which enciphers the generated session key Ks3 by the session key Ks2 obtained by the decode processing section 1206, and is outputted to a bus BS 2 is included.

[0110]

A portable telephone 100 contains further the decode processing section 1212 which decodes and outputs the data on a bus BS 2 by the session key Ks3.

[0111]

The decode processing section 1214 which decodes a portable telephone 100 further with the license key Kc acquired from the bus BS 2 from the decode processing section 1212 in response to encryption contents {data Data} Kc, and outputs contents data,
The music playback section 1216 for reproducing contents data in response to the output of the decode processing section 1214,
DA converter 1218 which changes the output of the music playback section 1216 into an analog signal from a digital signal,
The switch 1222 for outputting from a terminal 1114 or a terminal 1220 selectively in response to the output of DA converter 1113 and DA converter 1218 according to a mode of operation,
In response to the output of a switch 1222, the connection terminal 1224 for connecting with a head telephone 130 is included.

[0112]

In addition, in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000008"
TARGET="tjitemdrw">drawing 6</A>
, for the simplification of explanation, only the block in connection with distribution and playback of this invention of music data is indicated among portable telephones, and the publication is omitted in part about the block about the call function with which the portable telephone is originally equipped.

[0113]

About the actuation in each session of each component of a portable telephone 100, the back is explained to a detail using a flow chart.

[0114]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"
TARGET="tjitemdrw">Drawing 7</A>
is an outline block diagram for explaining the configuration of a memory card 110. Although KPmci and Kmci are prepared in a memory card and the class certificate Cmci of a memory card is formed in it as the open cryptographic key and secrecy decode key of a proper as already explained, in a memory card 110, these shall be expressed with the natural number i= 1, respectively.

[0115]

Therefore, the authentication data-hold section 1400 in which a memory card 110 holds the authentication data {KPmc1//Cmc1} KPma,
Kmc1 attaching part 1402 holding Kmc1 which is the decode key of the proper set up for every class of memory card,
Km1 attaching part 1421 holding the secrecy decode key Km1 set as a proper for every memory card and KPm1 attaching part 1416 holding the open cryptographic key KPm1 which can be decoded by Km1 are included.
authentication -- data-hold -- the section -- 1400 -- a memory card -- a class -- and -- a class -- every -- respectively -- setting up -- having -- secrecy -- a cryptographic key -- KPmc -- one -- and -- a class -- a certificate -- Cmc -- one --

disclosure -- authentication -- a key -- KPma -- decoding -- things -- the -- justification -- it can attest -- a condition -- having enciphered -- authentication -- data -- {-- KPmc -- one -- /-- /-- Cmc -- one --} -- KPma -- ****** -- holding .

[0116]

Thus, by preparing the cryptographic key of a recording device called a memory card, it becomes possible to perform management of the distributed contents data or the enciphered license key per memory card so that it may become clear by the following explanation.

[0117]

The interface 1423 with which a memory card 110 delivers further and receives a signal through a terminal 1201 between the memory interfaces 1200,
The bus BS 3 which exchanges a signal between interfaces 1423
The secrecy decode key Kmc1 of a proper is received from Kmc1 attaching part 1402 for every class of the data given to a bus BS 3 from an interface 1423 to memory card.
The decode processing section 1404 which outputs the session key Ks1 which the distribution server 30 generated in the distribution session to Contact Pa,
The decode processing section 1408 which performs decode processing by KPma from the data given to a bus BS 3 in response to the authentication key KPma from the KPma attaching part 1414, and outputs a decode result to the encryption processing section 1410,
The encryption processing section 1406 which enciphers the data selectively given by the change-over switch 1444, and is outputted to a bus BS 3 with the key selectively given by the change-over switch 1442 is included.

[0118]

The session key generating section 1418 in which a memory card 110 generates the session key Ks2 in each session of distribution and playback further,
The encryption processing section 1410 which enciphers the session key Ks2 which the session key generating section 1418 outputted by the open cryptographic keys KPpn and KPmci obtained by the decode processing section 1408, and is sent out to a bus BS 3,
It decodes by the session key Ks2 obtained from the session key generating section 1418 in response to the data enciphered by the session key Ks2 from the bus BS 3, and the decode processing section 1412 which sends out a decode result to a bus BS 4 is included.

[0119]

The decode processing section 1422 for a memory card 110 to decode the data on a bus BS 3 further with the open cryptographic key KPm1 and the secrecy decode key Km1 of memory card 110 proper which makes a pair,
While storing in response to the inhibited class list data CRL updated serially from a bus BS 4 by data CRL_dat for the renewal of a version of an inhibited class list Encryption contents data {Data} The memory 1415 for storing in response to Kc and additional information Data-inf from a bus BS 3 is included.
Memory 1415 is constituted by semiconductor memory.
Moreover, memory 1515 consists of data area 1415B which recorded CRL field 1415A which recorded the inhibited class list CRL, Header containing content ID, encryption contents {data Data} Kc, and related information Data-inf of encryption contents data.

[0120]

A memory card 110 contains the license information attaching part 1440 for holding further the license acquired by the decode processing section 1422, and the controller 1420 for performing data transfer between the exteriors through a bus BS 3, and controlling actuation of a memory card 110 in response to playback information etc. between buses BS 4.

[0121]

The license information attaching part 1440 has a bank of N individual (N: natural number), and holds the license corresponding to each license for every bank.

[0122]

In addition, in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"
TARGET="tjitemdrw">drawing 7</A>
, the field enclosed with a continuous line shall be included in the module TRM for making impossible read-out of the data in the circuit which exists in the field to a third party etc. by elimination of an in-house data, or destruction of an internal circuitry, if unjust opening processing from the outside etc. is performed in a memory card 110.
Generally such a module is a tamper resistance module (Tamper Resistance Module).

[0123]

Of course, it is good also as a configuration incorporated in Module TRM also including memory 1415.
However, since each playback information required for the playback currently held in memory 1415 by considering as a configuration as shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"
TARGET="tjitemdrw">drawing 7</A>
is data enciphered, since a third party does not need to form memory 1415 in an expensive tamper resistance module impossible as for playing music, he has the advantage that a manufacturing cost is reduced, only by the data in this memory 1415.

[0124]

Henceforth, for simplification, the access-control information AC 1 shall restrict only the playback length which is the control information which specifies the length when the regenerative-circuit control information AC 2 is refreshable only for the count of playback which is the control information which restricts the count of playback, and shall call the access-control information AC 1 and the regenerative-circuit control information AC 2 the count limit AC 1 of playback, and the playback length AC 2, respectively.

[0125]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
, various kinds of conditions in the memory card 110 on which encryption contents {data Data} Kc and the license which consists of the license key Kc, the count limit AC 1 of playback, and playback length AC2 grade were recorded are explained.
In addition, in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
, the case where there is no limit in the count limit AC 1 of playback is expressed with "FF", and the case where there is no limit in the playback length AC 2 is expressed with "00."
Encryption contents {data Data} Kc and a license are recorded on the memory card 110, and (a) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B

%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
shows the case where encryption contents {data Data} Kc and a license are newly received from the distribution server 30.
Moreover, encryption contents {data Data} Kc and the license key Kc exist, and (b) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
shows the case where playback of encryption contents {data Data} Kc is restricted by the part and the count limit AC 1 of playback.
Furthermore, encryption contents {data Data} Kc and a license are recorded, and (c) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
shows the case where the license which reproduces a part of encryption contents {data Data} Kc(s) is not recorded.

[0126]

Encryption contents data:{Data(55019930112)} Kc specified by content ID:55019930112, and 55019951013 and 55019630122 with reference to (a) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
(55019930112),
{Data (55019951013)} Kc (55019951013),
{Data (55019630122)} Kc (55019630122),
The license key for decoding the encryption contents data: AAF53951046FD356ABCC, 96F539510456AB332C55, and F6F53695104AF3323C31 are recorded.
Moreover, content ID: Although the encryption contents data specified by 55019951013 and 55019630122 have the count limit AC 1 of playback, and the unrestricted playback length AC 2, the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 20 times.
Therefore, the license over three encryption contents {data Data} Kc(s) recorded on data area 1415B is recorded on the license information attaching part 1440.

[0127]

(b) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
-- referring to -- content ID: -- license key:AAF53951046FD356ABCC for decoding encryption contents data:{Data(55019930112)} Kc (55019930112) specified by 55019930112 and 55019951013, {Data(55019951013)} Kc (55019951013), and its encryption contents data and 96F539510456AB332C55 are recorded.
Moreover, content ID: Although the encryption contents data specified by 55019951013 have the count limit AC 1 of playback, and the unrestricted playback length AC 2, the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 0 times.
Therefore, as for one encryption contents data, the license is not recorded on the license information attaching part 1440 between two encryption contents {data Data} Kc(s) recorded on data area 1415B.

[0128]

(c) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
-- referring to -- content ID: -- license key:AAF53951046FD356ABCC for decoding encryption contents data:{Data(55019930112)} Kc (55019930112) specified by 55019930112 and 55019951013, {Data(55019951013)} Kc (55019951013), and its encryption contents data and 96F539510456AB332C55 are recorded.
Moreover, content ID: The encryption contents data specified by 55019951013 have the count limit AC 1 of playback, and the unrestricted playback length AC 2, and the playback length AC 2 of the count limit AC 1 of playback of the encryption contents data specified by content ID:55019930112 is unrestricted 20 times.
Furthermore, content ID: Although encryption contents data:{Data(55019630122)} Kc (55019630122) specified by 55019630122 is recorded on data area 1415B, the license which consists of the license key Kc for reproducing the encryption contents data, the count limit AC 1 of playback, and the playback length AC 2 is not recorded on the license information attaching part 1440.
Therefore, the license over one encryption contents data does not exist among three encryption contents {data Data} Kc(s) recorded on data area 1415B.

[0129]

As explained with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
, various kinds of conditions exist in a memory card 110 by whether the encryption contents data {Data} Kc, the license key Kc, the count limit AC 1 of playback, and the playback length AC 2 are recorded.

[0130]

Next, a portable telephone 100 is equipped with the memory card 110 on which encryption contents {data Data} Kc, the license key Kc, etc. were recorded in various kinds of condition, and actuation when request to receipt of encryption contents data is carried out from the user of a portable telephone 100 is explained.

[0131]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">Drawing 9</A>
-
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014"
TARGET="tjitemdrw">drawing 12</A>
are the 1st for explaining the distribution actuation (henceforth a distribution session) generated at the time of the purchase of the encryption contents data in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
- the 4th flow chart.

[0132]

If the distribution demand of contents data is made through the key stroke section 1108 with reference to
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011" TARGET="tjitemdrw">drawing 9</A>
from the user of a portable telephone 100, a portable telephone 100 will transmit the Request to Send of a contents menu to the distribution server 30 (step S70).
If the Request to Send of a contents menu is received through a communication device 350 and a bus BS 1 (step S72), from the menu database 307, read-out will be minded for a contents menu, and the distribution control section 315 of the distribution server 30 will mind a bus BS 1 and a communication device 350 for the read contents menu through a bus BS 1, and will transmit to a portable telephone 100 (step S74).
A portable telephone 110 receives a contents menu by the transceiver section 1104, and a controller 1106 displays a contents menu on a display 1110 (step S76).

[0133]

If it does so, the contents menu 60 shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000015" TARGET="tjitemdrw">drawing 13</A>
will be displayed on the display 1110 of a portable telephone 100.
A user chooses the numbers 001, 002, and 003 of the contents menu 60, and the encryption contents data which wish to distribute by choosing ...
The shift section 1111 for shifting to another screen is formed in the display 1110.
A user clicks the shift section 1111, when the encryption contents data wished to have into the contents menu 60 displayed on the display 1110 are not displayed.
The address for shifting to another screen is included in the shift section 1111.

[0134]

It is required that a controller 1106 will transmit the address included in the shift section 1111 to the distribution server 30 through the transceiver section 1104, and the controller 1106 of a portable telephone 100 will transmit another screen if it judges whether it is the no as which contents were chosen (step S78) and the shift section 1111 is clicked.
And steps S70-S78 are repeated.
That is, two or more screens which consist of the contents menu 60 are arranged hierarchical, the contents menu is constituted, and although each screen is the encryption contents data and the same genre from which a genre differs, it is constituted by the contents menu which consists of other encryption contents data etc.

[0135]

And when the encryption contents data to wish to have are not contained in the contents menu sent by two or more screens from the distribution server 30, distribution actuation shifts to step S170, and distribution actuation is ended.

[0136]

The contents menu 60 contains the content ID for specifying encryption contents data, and when encryption contents data are chosen in step S78, the content ID of the encryption contents data chosen from the contents menu is extracted (step S80).

[0137]

And the purchase conditions AC for purchasing the license of encryption contents data through the key stroke section 1108 are inputted (step S82).
That is, in order to purchase the license key Kc which decodes selected encryption contents data, the count limit AC 1 of playback and the playback length AC 2 of encryption contents data are set up, and the purchase conditions AC are inputted.

[0138]

If the purchase conditions AC of encryption contents data are inputted, a controller 1106 will search whether encryption contents {data Data} Kc which has the same content ID as the content ID to selected encryption contents data is recorded on the memory card 110 (step S84).
In this case, a controller 1106 transmits the content ID corresponding to selected encryption contents data to a memory card 110 through the memory interface 1200. The controller 1420 of a memory card 110 searches whether the encryption contents data as which the user chose content ID from the contents menu by whether it is in agreement with the content ID by which a receipt and its received content ID are contained in Header1424 of memory 1415 are recorded on the memory card 110 from the portable telephone 100 through the interface 1423 and the bus BS 3.

[0139]

In this case, if signature data using the Hash Function etc. considering Header and Data-inf which were recorded on the memory 1415 of a memory card 110, and {Data} Kc as one data stream are collectively dealt with as shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000016"
TARGET="tjitemdrw">drawing 14</A>
, reorganization of content ID can be prevented.
What is necessary is just to perform the check of a signature also about the thing corresponding to the time of inspection of content ID.

[0140]

And a controller 1106 stands flag "Yes" for acquiring data from the distribution server 30, when it judges whether selected encryption contents data are recorded on the memory card 110 (step S86) and encryption contents data are not recorded on a memory card 110 (step S88).
The check of a license is performed when encryption contents data are recorded on the memory card 110 (step S90).
That is, the check of a license is performed by whether the license key Kc is recorded on the memory card 110 as having explained with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">drawing 8</A>
, or playback of encryption contents data is not restricted by the count limit AC 1 of playback, and the playback length AC 2.
When a license does not exist, it shifts to step S94.
When a license exists and encryption contents data can be reproduced, a controller 1106 displays "license simple substance purchase ?" on a display 1110, and it is sure of the intention of whether to purchase only a license alone (step S92).
If directions of the purport which does not purchase only a license are inputted from the key stroke section 1108, a controller 1106 will shift to step S170, and will end distribution actuation of encryption contents data.
A controller 1106 will stand flag "No" which does not acquire data from the distribution server 30, if directions of the purport which purchases only a license alone are inputted from the key stroke section 1108 (step S94).

[0141]

Next, with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000012"
TARGET="tjitemdrw">drawing 10</A>
, the distribution request by assignment of content ID (step S80 reference) that the user extracted the portable telephone 100 by choosing encryption contents data is made (step S100).

[0142]

In a memory card 110, the authentication data {KPmc1//Cmc1} KPma are outputted from the authentication data-hold section 1400 according to this distribution request (step S102).

[0143]

In addition to the authentication data KPma for the authentication from a memory card 110 {KPmc1//Cmc1}, a portable telephone 100 transmits the data AC of content ID and license purchase conditions to the distribution server 30 (step S104).

[0144]

In the distribution server 30, content ID, the authentication data {KPmc1//Cmc1} KPma, and the data AC of license purchase conditions are received from a portable telephone 100 (step S106), and decode processing is performed for the authentication data outputted from the memory card 110 in the decode processing section 312 with the open authentication key KPma (step S108).

[0145]

The distribution control section 315 performs authentication processing which judges whether the authentication data which gave the code for proving the justification in the engine of normal were received, in order to attest that whether processing having been performed normally and a memory card 110 hold the open cryptographic key KPmc1 and certificate Cmc1 from a memory card of normal from the decode processing result in the decode processing section 312 (step S110).
When it is judged that it is just authentication data, the distribution control section 315 recognizes and receives the open cryptographic key KPmc1 and a certificate Cmc1.
And it shifts to the next processing (step S112).
In not being just authentication data, it supposes un-recognizing, and it ends processing without receiving the open cryptographic key KPmc1 and a certificate Cmc1 (step S170).

[0146]

If it is recognized as a result of authentication that it is the device of normal, when, as for the distribution control section 315, these class certificates are set as the object of an inhibited class list by referring for whether next the class certificate Cmc1 of a memory card 110 is listed by the inhibited class list CRL to the CRL database 306, a distribution session is ended here (step S170).

[0147]

On the other hand, when the class certificate of a memory card 110 is outside the object of an inhibited class list, it shifts to the next processing (step S112).

[0148]

If it is checked that it is access from the portable telephone equipped with a memory card with just authentication data as a result of authentication, and a class is outside the object of an inhibited class list, in the distribution server 30, the distribution control section 315 will generate the transaction ID which is Control Code for specifying distribution (step S113).
Moreover, the session key generating section 316 generates the session key Ks1 for distribution.
The session key Ks1 is enciphered by the encryption processing section 318 by the open cryptographic key KPmc1 corresponding to the memory card 110 obtained by the decode processing section 312 (step S114).

[0149]

Transaction ID and the enciphered session key Ks1 are outputted outside through a bus BS 1 and a communication device 350 as transaction ID//{Ks1} Kmc1 (step S116).

[0150]

When the decode processing section 1404 carries out decode processing of the received data with which it was given to the bus BS 3 through the memory interface 1200 in the memory card 110 when the portable telephone 100 received transaction

ID//{Ks1} Kmc1 (step S118) with the secrecy decode key Kmc1 of memory card 110 proper held at an attaching part 1402, the session key Ks1 is decoded and extracted (step S120).

[0151]

A controller 1420 directs generation of the session key Ks2 generated in a memory card 110 at the time of distribution actuation to the session key generating section 1418, if acceptance of the session key Ks1 generated by the distribution server 30 is checked.

[0152]

Moreover, in a distribution session, a controller 1420 extracts data CRL_dat of the inhibited class list currently recorded on the memory 1415 in a memory card 110 from memory 1415, and outputs it to a bus BS 4.

[0153]

By the session key Ks1 given from the decode processing section 1404 through the contact Pa of a change-over switch 1442, the encryption processing section 1406 enciphers data CRL_dat of the session key Ks2 given by switching the contact of change-over switches 1444 and 1446 one by one, the open cryptographic key KPm1, and an inhibited class list as one data stream, and outputs {Ks2//KPm1//CRL_dat} Ks1 to a bus BS 3 (step S122).

[0154]

Encryption data {Ks2//KPm1//CRL_ver} Ks1 outputted to the bus BS 3 is outputted to a portable telephone 100 through an interface 1423, a terminal 1201, and the memory interface 1200 from a bus BS 3, and is transmitted to the distribution server 30 from a portable telephone 100 (step S124).

[0155]

The distribution server 30 receives transaction ID//{Ks2//KPm1//CRL_dat} Ks1, performs decode processing by the session key Ks1 in the decode processing section 320, and receives data CRL_dat of the inhibited class list in the open cryptographic key KPm1 and memory card 110 of the session key Ks2 and memory card 110 proper which were generated by the memory card 110 (step S126).

[0156]

The distribution control section 315 generates License ID, the access-restriction information AC 1, and the playback length AC 2 according to the data AC of the content ID acquired at step S106, and license purchase conditions (step S128). Furthermore, the license key Kc for decoding encryption contents data is acquired from the information database 304 (step S130).

[0157]

The distribution control section 315 gives the generated license Kc, i.e., a license key, the playback length AC 2, License ID, content ID, and the access-restriction information AC 1 to the encryption processing section 326.
The encryption processing section 326 shifts to step S134, when it is judged for data CRL_dat of the inhibited class list transmitted from the memory card 110 by the open cryptographic key KPm1 of memory card 110 proper obtained by the decode processing section 320 in the distribution server 30 whether it is the newest and data CRL_dat is judged to be the newest with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000013"
TARGET="tjitemdrw">drawing 11</A>
(step S132) which enciphers a license.
Moreover, when data CRL_dat is not the newest, it shifts to step S137 (step S133).

[0158]

When data CRL_dat is judged to be the newest, the encryption processing section 328 Encryption data {Kc//AC2// license ID// content ID// AC1} outputted from the

encryption processing section 326 Km1 is enciphered by the session key Ks2 generated in the memory card 110.
Encryption data {Kc//AC2// license ID// content ID// {AC1} Km1} Ks2 is outputted to a bus BS 1.
And the distribution control section 315 transmits Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 on a bus BS 1 to a portable telephone 100 through a communication device 350 (step S134).

[0159]

And a portable telephone 100 receives Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 (step S135), and transmits it to a memory card 110 through a bus BS 2 and the memory interface 1200.
The decode processing section 1412 of a memory card 110 decodes Kc//AC2// license ID// content ID// encryption data {{AC1} Km1} Ks2 by the session key Ks2 generated by the receipt and the session key generating section 1418 through the terminal 1201 and the interface 1423, and receives Kc//AC2// license ID// content ID// {AC1} Km1 (step S136).
Then, it shifts to step S146.

[0160]

On the other hand, if it is judged in the distribution server 30 that CRL_dat is not the newest, the distribution control section 315 will acquire data CRL_dat of the newest inhibited class list from the CRL database 306 through a bus BS 1 (step S137).

[0161]

The encryption processing section 328 is enciphered by the session key Ks2 generated in the memory card 110 in response to the output of the encryption processing section 326, and newest data CRL_dat of the inhibited class list which the distribution control section 315 supplies through a bus BS 1.
The encryption data outputted from the encryption processing section 328 are transmitted to a portable telephone 100 through a bus BS 1 and a communication device 350 (step S138).

[0162]

Thus, by exchanging the cryptographic key generated by the distribution server and the memory card, respectively, performing encryption using the cryptographic key which each received, and transmitting the encryption data to the other party, mutual recognition on data can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.

[0163]

A portable telephone 100 receives transmitted encryption data {Kc//AC2// license ID// content ID// {AC1} Km1//CRL_dat} Ks2 (step S140), and outputs it to a memory card 110 through the memory interface 1200.
In a memory card 110, the received data given to the bus BS 3 are decoded by the decode processing section 1412 through a terminal 1201 and an interface 1423.
The decode processing section 1412 decodes the received data of a bus BS 3 using the session key Ks2 given from the session key generating section 1418, and outputs them to a bus BS 4 (step S142).

[0164]

In this phase, encryption {license AC 1} Kc//AC2// license ID// content ID// Km1 which can be decoded with the secrecy decode key Km1 held at Km1 attaching part 1421, and CRL_dat are outputted to a bus BS 4 (step S142).
The inhibited class list CRL of [in memory 1415] is rewritten by the newest inhibited class list CRL_dat received with directions of a controller 1420 (step S144).

[0165]

Steps S134, S135, and S136 are distribution actuation to the memory cards 110, such as the license key Kc in case inhibited class list CRL_dat sent from the memory card 110 is the newest, and steps S137, S138, S140, S142, and S144 are distribution

actuation to the memory cards 110, such as the license key Kc in case inhibited class list CRL_dat sent from the memory card 110 is not the newest.
Thus, when checking in detail and not updating whether inhibited class list CRL_dat sent from the memory card 110 is updated,
By acquiring the newest inhibited class list CRL_dat from the CRL database 306, and distributing to a memory card 110
The playback of encryption contents {data Data} Kc by the portable telephone with which the distribution of encryption contents {data Data} Kc to the memory card by which the license was broken was prevented, and the license was broken can be prevented.

[0166]

After step S136 or step S144, encryption {license AC 1} Kc//AC2// license ID// content ID// Km1 are decoded by directions of a controller 1420 with the secrecy decode key Km1 in the decode processing section 1422, and a license (the license key Kc, License ID, content ID, the count limit AC 1 of playback, and playback length AC 2) is received by them (step S148).

[0167]

A controller 1420 records a license on the license information attaching part 1440 (step S150).

[0168]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014"
TARGET="tjitemdrw">drawing 12</A>
, the controller 1106 of a portable telephone 100 judges whether encryption contents data are acquired from the distribution server 30 with reference to the flag set in step S88 and step S94.
And when not acquiring encryption contents data from the distribution server 30, it shifts to step S164, and when acquiring encryption contents data from the distribution server 30, it shifts to step S154.

[0169]

When acquiring encryption contents data from the distribution server 30, a portable telephone 100 transmits the distribution demand of the Transaction ID and encryption contents data which were sent from the distribution server 30 to the distribution server 30 (step 154).

[0170]

The distribution server 30 receives the distribution demand of Transaction ID and encryption contents data (step S156), from the information database 304, acquires encryption contents {data Data} Kc and additional information Data-inf, and outputs these data through a bus BS 1 and a communication device 350 (step S158).

[0171]

A portable telephone 100 receives {Data} Kc//Data-inf, and receives encryption contents {data Data} Kc and additional information Data-inf (step S160).
Encryption contents data {Data} Kc and additional information Data-inf are transmitted to the bus BS 3 of a memory card 110 through the memory interface 1200, a terminal 1201, and an interface 1423.
In a memory card 110, encryption contents {data Data} Kc and additional information Data-inf which received are recorded on memory 1415 as it is (step S162).

[0172]

It includes, also when it is judged that encryption contents data are not received from the distribution server 30 in step S152. And to the distribution server 30, from a memory card 110
Advice of transaction ID// distribution acceptance is transmitted (step S164).
If transaction ID// distribution acceptance is received by the distribution server

30 (step S166)
Storing of the account data to the accounting database 302 and record in the distribution record database 308 of Transaction ID are performed, processing of distribution termination is performed (step S168), and the whole processing is completed (step S170).

[0173]

Thus, the memory card 110 with which the portable telephone 100 was equipped is the device of normal,
After checking that the open cryptographic keys Kp1 and Kmc1 which have enciphered and transmitted with the class certificate Cmc1 are effective simultaneously
Each class certificate Cmc1 can distribute contents data only to the distribution demand from the memory card which is not indicated by the inhibited class list, i.e., the class certificate list with which encryption by the open cryptographic keys Kp1 and Kmc1 was broken.
The distribution using the class key to an inaccurate memory card distributed and decoded can be forbidden.

[0174]

Moreover, according to the record situation of the encryption contents {data Data} encryption contents data {Data} Kc in a memory card 110 to the distribution server 30, the license key Kc, and count limit ACof playback 1 grade, only required distribution can be required of the distribution demand of Kc at the distribution server 30.
Consequently, useless distribution can be prevented.

[0175]

Next, the playback actuation in the portable telephone 100 of the contents data distributed to the memory card 110 with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"
TARGET="tjitemdrw">drawing 15</A>
and
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000018"
TARGET="tjitemdrw">drawing 16</A>
is explained.
With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"
TARGET="tjitemdrw">drawing 15</A>
, playback directions are inputted to a portable telephone 100 through the key stroke section 1108 with initiation of playback actuation from the user of a portable telephone 100 (step S200).
If it does so, a controller 1106 will input the authentication data {KPp1//Crtf1} KPma into a memory card 110 for the authentication data {KPp1//Crtf1} KPma through read-out and the memory interface 1200 through a bus BS 2 from the authentication data-hold section 1202 (step S201).

[0176]

If it does so, a memory card 110 will receive the authentication data {KPp1//Crtf1} KPma (step S202).
And the decode processing section 1408 of a memory card 110 decodes the received authentication data {KPp1//Crtf1} KPma with the open authentication key KPma held at the KPma attaching part 1414 (step S203), and a controller 1420 performs authentication processing from the decode processing result in the decode processing section 1408.

That is, authentication processing which judges whether the authentication data {KPp1//Crtf1} KPma are authentication data of normal is performed (step S204).
When it is not able to decode, a controller 1420 outputs authentication data a non-received output to the memory interface 1200 of a portable telephone 100 through data BS 3 and a terminal 1201 (step S206).
When authentication data are able to be decoded, it judges whether a controller 1420 is contained in the inhibited class list data which the acquired certificate Crtf1 read from memory 1415 (step S205).
In this case, ID is given to the certificate Crtf1 and a controller 1420 distinguishes whether ID of the received certificate Crtf1 exists in inhibited class list data.
If a certificate Crtf1 is judged to be contained in inhibited class list data, a controller 1420 will output authentication data a non-received output to the memory interface 1200 of a portable telephone 100 through data BS 3 and a terminal 1201 (step S206).

[0177]

When authentication data are not able to decode with the open authentication key KPma in step S204, and when the certificate Crtf1 received in step S205 is contained in inhibited class list data, authentication data a non-received output is made.
And the controller 1106 of a portable telephone 100 will display authentication data non-received data on a display 1110, if authentication data a non-received output is undergone through the memory interface 1200 (step S207).

[0178]

In step S205, if a certificate Crtf1 is judged not to be contained in inhibited class list data, with reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000018"
TARGET="tjitemdrw">drawing 16</A>
, the session key generating section 1418 of a memory card 110 will generate the session key Ks2 for playback sessions (step S208).
And the cipher-processing section 1410 outputs {Ks2} Kp1 which enciphered the session key Ks2 from the session key generating section 1418 by the open cryptographic key KPp1 decoded in the decode processing section 1408 to a bus BS 3 (step S209).
If it does so, a controller 1420 will output {Ks2} Kp1 to the memory interface 1200 through a terminal 1201, and the controller 1106 of a portable telephone 100 will acquire {Ks2} Kp1 through the memory interface 1200.
And Kp1 attaching part 1204 outputs the secrecy decode key Kp1 to the decode processing section 1206.

[0179]

With the secrecy decode key Kp1 which was outputted from Kp1 attaching part 1204 and which is the open cryptographic key KPp1 and a pair, the decode processing section 1206 decodes {Ks2} Kp1, and outputs the session key Ks2 to the cipher-processing section 1208 (step S210).
If it does so, the session key generating section 1210 will generate the session key Ks3 for playback sessions, and will output the session key Ks3 to the cipher-processing section 1208 (step S211).
The cipher-processing section 1208 enciphers the session key Ks3 from the session key generating section 1210 by the session key Ks2 from the decode processing section 1206, and outputs {Ks3} Ks2, and a controller 1106 outputs {Ks3} Ks2 to a memory card 110 through a bus BS 2 and the memory interface 1200 (step S212).

[0180]

The decode processing section 1412 of a memory card 110 inputs {Ks3} Ks2 through a terminal 1201, an interface 1423, and a bus BS 3, decodes {Ks3} Ks2 by the session key Ks2 generated by the session key generating section 1418, and acquires the session key Ks3 generated in the portable telephone 100 (step S213).

[0181]

According to acceptance of the session key Ks3, a controller 1420 checks the access-restriction information AC 1 to which it corresponds in the license information attaching part 1440 (step S214).

[0182]

In step S214, by checking the access-restriction information AC 1 which is the information about the limit to access of memory, it ends playback actuation, in being in a condition [that it is already unreproducible], and it progresses to the following step, after updating the data of the access-restriction information AC 1 and updating the count of refreshable, when the count limit of playback has a limit (step S215).
On the other hand, when the count limit of playback is not restricted by the access-restriction information AC 1, step S215 is skipped, and processing advances to the following step (step S216), without updating the count limit AC 1 of playback.

[0183]

Moreover, when the content ID concerned of a request song does not exist in the license information attaching part 1440, it judges that it is in a condition [being unreproducible], and playback actuation is ended.

[0184]

In step S214, when it is judged in the playback actuation concerned that it is reproducible, the license key Kc of a playback request song and the playback length AC 2 which were recorded on the license information attaching part 1440 are outputted on a bus BS 4 (step S216).

[0185]

The license key Kc and the playback length AC 2 which were obtained are sent to the encryption processing section 1406 through the contact Pd of a change-over switch 1444.
Through the contact Pd of a change-over switch 1442, by the carrier beam session key Ks3, the encryption processing section 1406 enciphers the carrier beam license key Kc and the playback length AC 2 from a bus BS 4, and outputs {Kc//AC2} Ks3 to a bus BS 3 from the decode processing section 1412 (step S217).

[0186]

The encryption data outputted to the bus BS 3 are sent out to a portable telephone 100 through an interface 1423, a terminal 1202, and the memory interface 1200.

[0187]

In a portable telephone 100, the decode processing section 1212 performs decode processing for encryption {Kc// data AC 2} Ks3 transmitted to a bus BS 2 through the memory interface 1200, and the license key Kc and the playback length AC 2 are received (step S218).
The decode processing section 1212 transmits the license key Kc to the decode processing section 1214, and outputs the playback length AC 2 to a bus BS 2.

[0188]

Through a bus BS 2, a controller 1106 receives the playback length AC 2, and checks reproductive propriety (step S219).

[0189]

In step S219, when it is judged by the playback length AC 2 that playback is impossible, playback actuation is ended.

[0190]

When it is judged in step S219 that it is refreshable, a controller 1106 requires encryption contents {data Data} Kc of a memory card 110 through the memory interface 1200.
If it does so, the controller 1420 of a memory card 110 will acquire encryption contents {data Data} Kc from memory 1415, and will output it to the memory interface

1200 through a bus BS 3 and a terminal 1201 (step S220).

[0191]

The controller 1106 of a portable telephone 100 acquires encryption contents {data Data} Kc through the memory interface 1200, and gives encryption contents {data Data} Kc to the decode processing section 1214 through a bus BS 2.
And the decode processing section 1214 decodes encryption contents {data Data} Kc with the contents key Kc outputted from the decode processing section 1212, and acquires the contents data Data (step S221).

[0192]

And they are outputted to the music playback section 1216, and the decoded contents data Data reproduce contents data, and the music playback section 1216 changes a digital signal into an analog signal, and outputs DA converter 1218 to a terminal 1220.
And a switch 1222 chooses a terminal 1220, and through a terminal 1224, music data are outputted to a head telephone 130, and are reproduced (step S222).
Playback actuation is completed by this.

[0193]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">drawing 17</A>
, the example of distribution, such as encryption contents {data Data} Kc, the license key Kc, etc. according to record situations, such as encryption contents {data Data} Kc in a memory card 110 and the license key Kc, is explained.
With reference to (a) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">drawing 17</A>
, encryption contents data:{Data(55019930112)} Kc (55019930112), {Data(55019951013)} Kc (55019951013), {Data(55019630122)} Kc (55019630122), and each related information Data-inf are recorded on data area 1415B of a memory card 110.
Moreover, the license LS 1 of content ID:55019930112, transaction ID:000000000001, license key Kc:AAF53951046FD356ABCC, the count limit AC 1:00 of playback, and the playback length AC 2:00 and the license LS 2 of content ID:55019951013, transaction ID:000000003005, license key Kc:96F539510456AB332C55, count limit ACof playback1:FF, and the playback length AC 2:00 are recorded on license field 1415A.
And about the license LS 1, since the count limit AC 1 of playback is "00", encryption contents {data Data (55019930112)} Kc (55019930112) cannot be reproduced, namely, the condition that there is no license is shown.
Moreover, about encryption contents {data Data (55019630122)} Kc (55019630122), content ID, the license key Kc, the count limit AC 1 of playback, and the playback length AC 2 are not recorded, but the condition that there is no license is shown.
That is, the license LS 2 over encryption contents {data Data (55019951013)} Kc (55019951013) exists, and they are encryption contents {data Data (55019930112)} Kc (55019930112) and {Data (55019630122} it is in the situation that the license over Kc (55019630122) does not exist.).

[0194]

In the situation of a memory card 110 shown in (a) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">drawing 17</A>
, if the distribution demand of encryption contents {data Data} Kc specified by content ID:55019930112 from the user of a portable telephone 100 is inputted through

the key stroke section 1108, steps S70-S78 of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
will be performed, and content ID:55019930112 will be extracted (step S80).
And in step S82, the purchase conditions AC of the license made refreshable to "20" times are inputted.
And content ID: It is searched whether encryption contents {data Data} Kc specified by 55019930112 is recorded on the memory card 110 (step S84).

[0195]

In this case, content ID: Since encryption contents {data Data} Kc specified by 55019930112 is recorded on the memory card 110 as encryption contents {data Data (55019930112)} Kc (55019930112), it shifts to step S90 through step S86 of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
.
And in step S90, it is judged according to a license whether encryption contents {data Data (55019930112)} Kc (55019930112) is refreshable.
In this case, since the count limit AC 1 of playback is "00", encryption contents {data Data (55019930112)} Kc (55019930112) is unreproducible.
Therefore, it shifts to step S94 from step S90.
And after the flag of data acquisition ="No" is set in step S94, only the license which makes "20" times the count limit AC 1 of playback by step S100 - step S170 is distributed to a memory card 110 from the distribution server 30.
And as shown in (b) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">drawing 17</A>
, the count limit AC 1 of playback of license LS 1 is changed with "20."
Encryption contents {data Data (55019930112)} Kc (55019930112) is [with this] reproducible with license LS 1.

[0196]

Moreover, in the situation of a memory card 110 shown in (a) of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">drawing 17</A>
, if the distribution demand of encryption contents {data Data} Kc specified by content ID:55012345678 from the user of a portable telephone 100 is inputted through the key stroke section 1108, steps S70-S78 of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
will be performed, and content ID:55012345678 will be extracted (step S80).
then -- as the purchase conditions AC for a license -- AC1: -- those of FF and AC2:00 without a playback limit are inputted (step S82).
And content ID: It is searched whether encryption contents {data Data} Kc specified by 55012345678 is recorded on the memory card 110 (step S84).
In this case, content ID: Since encryption contents {data Data} Kc specified by 55012345678 is not recorded on a memory card 110, from step S86, it shifts to step

S88 and the flag of data acquisition ="Yes" is set in step S88.

[0197]

Then, step S100 - step S170 are performed, and content ID:55012345678, transaction ID:000005500345, license key Kc:C6F569510456AB333C4, count limit ACof playback1:FF, the playback length AC 2:00, encryption contents data:{Data(55012345678)} Kc (55012345678), and related information DataD-inf (55012345678) are distributed and recorded on a memory card 110.
By this, a memory card 110 will be in the condition which shows in (c) of
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019" TARGET="tjitemdrw">drawing 17</A>
, and will become reproducible [encryption contents {data Data (55012345678)} Kc (55012345678) to which the user gave the distribution demand].

[0198]

Furthermore, in the situation of a memory card 110 shown in (a) of
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019" TARGET="tjitemdrw">drawing 17</A>
, if the distribution demand of encryption contents {data Data} Kc specified by content ID:55019630122 from the user of a portable telephone 100 is inputted through the key stroke section 1108, steps S70-S78 of
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011" TARGET="tjitemdrw">drawing 9</A>
will be performed, and content ID:55019630122 will be extracted (step S80).
then -- as the purchase conditions AC for a license -- AC1: -- those of FF and AC2:00 without a playback limit are inputted (step S82).
And content ID: It is searched whether encryption contents {data Data} Kc specified by 55019630122 is recorded on the memory card 110 (step S84).
In this case, content ID: Since encryption contents {data Data} Kc specified by 55019630122 is recorded on the memory card 110, shift to step S90 from step S86.
And in step S90, it is judged according to a license whether encryption contents {data Data (55019630122)} Kc (55019630122) is refreshable.
In this case, since neither content ID nor the license key Kc nor the count limit AC 1 of playback nor the playback length AC is recorded on the memory card 110, encryption contents {data Data (55019630122)} Kc (55019630122) is unreproducible.
Therefore, it shifts to step S94 from step S90.

[0199]

And after the flag of data acquisition ="No" is set in step S94, only the license made to have no playback limit by step S100 - step S170 is distributed to a memory card 110 from the distribution server 30.
And as shown in (d) of
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019" TARGET="tjitemdrw">drawing 17</A>
, content ID:55019630122, transaction ID:000000550339, license key Kc:F6F53695104AF3323C31, count limit ACof playback1:FF, and playback length:00 are recorded on license field 1415A of a memory card 110.
Encryption contents {data Data (55019630122)} Kc (55019630122) is reproducible with this.

[0200]

As mentioned above, according to record situations, such as encryption contents {data Data} Kc in a memory card 110, and the license key Kc, the user of a portable telephone 100 receives encryption contents {data Data} Kc, the license key Kc, etc. from the distribution server 30 to a memory card 110 using a portable telephone 100, can decode encryption contents {data Data} Kc with the license key Kc, and can be reincarnated.

[0201]

When the user of a portable telephone 100 performs the distribution demand of encryption contents {data Data} Kc in the above,
Although it was explained that encryption contents {data Data} Kc currently recorded on the memory card 110 was encryption contents data received from the distribution server 30
In this invention, not only this case but when only encryption contents {data Data} Kc is received from other than distribution server 30 and it records on a memory card 110, it is contained.

[0202]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
and
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"
TARGET="tjitemdrw">drawing 19</A>
, encryption contents {data Data} Kc is received from equipments other than distribution server 30, and the case where the encryption contents {data Data} Kc is recorded on a memory card 110 is explained.

[0203]

With reference to
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
, distribution of encryption contents {data Data} Kc using a computer 140 is explained.
To a portable telephone 100, a memory card 110 is removable, and the headphone 130 for playing music are connected.
And the portable telephone 100 is connected with the computer 140 through the telecommunication cable 145.

[0204]

A computer 140 is equipped with a hard disk 141, a controller 142, and an external interface 143.
And a hard disk 141 is connected with a controller 142 through a bus BS 5, and a controller 142 contains the license protection module 143.

[0205]

A hard disk 141 memorizes encryption contents {data Data} Kc distributed to the computer 140 through a bus BS 5 by the Internet distribution.
If a controller 142 has the Request to Send of encryption contents {data Data} Kc through a telecommunication cable 145 and an external interface 143 from the user of a portable telephone 100, it will output encryption contents {data Data} Kc to the exterior through read-out and an external interface 143 from a hard disk 141.

[0206]

An external interface 143 outputs the signal from a controller 142 to the exterior while inputting into a controller 142 the signal inputted into the computer 140 through the telecommunication cable 145 from the portable telephone 100.

[0207]

The license protection module 144 has the same configuration as the data-processing section 310 shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000007"
TARGET="tjitemdrw">drawing 5</A>
, exchanging a portable telephone 100 and a memory card 110, a open cryptographic key, a session key, etc., as mentioned above, in order to transmit encryption contents {data Data} Kc to the memory card 110 with which the portable telephone 100 was equipped, protects encryption contents {data Data} Kc, and transmits it to a memory card 110.

[0208]

Encryption contents {data Data} Kc is distributed to a computer 140 by the Internet distribution from a distribution server, and encryption contents data are memorized by the hard disk 141 of a computer 140 through the bus BS 5 by it.

[0209]

If the user of a portable telephone 100 inputs a Request to Send from the key stroke section 1108, a Request to Send will be inputted into a controller 142 through a telecommunication cable 145 and an external interface 143.
A controller 142 will input demanded encryption contents {data Data} Kc into read-out and the license protection module 144 from a hard disk 141 through a bus BS 5, if a Request to Send is received.

[0210]

The license protection module 144 exchanges a open cryptographic key, a session key, etc. through a memory card 110 and a telecommunication cable 145, as mentioned above, and it transmits encryption contents {data Data} Kc to a memory card 110.

[0211]

After transmission, by the same approach as having mentioned above, the user of a portable telephone 100 has the license (content ID, the license key Kc, the count limit AC 1 of playback, and playback length AC 2) of encryption contents {data Data} Kc distributed from the distribution server 30, and reproduces encryption contents {data Data} Kc.

[0212]

When CD is used, once after recording encryption contents {data Data} Kc which acquired from Music CD and was generated on a hard disk 141, it may transmit to a memory card 110, and may transmit to a memory card 110 directly, without transmitting to a hard disk 141.

[0213]

Encryption contents data {Data} As shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"
TARGET="tjitemdrw">drawing 19</A>
, Kc may equip a computer 140 with a memory card 110 directly, and may record encryption contents {data Data} Kc on a memory card 110.
In this case, the controller 142 of a computer 140 records encryption contents data on a memory card 110 directly with the license protection module 144.

[0214]

Also in

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"
TARGET="tjitemdrw">drawing 19</A>
, a computer 140 acquires encryption contents {data Data} Kc by the same approach as the case where it is shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">drawing 18</A>
.

[0215]

The portable telephone 100 of the flow chart in the case of performing a distribution demand of the license containing the license key corresponding to encryption contents {data Data} Kc which newly received to the distribution server 30, and the flow chart which reproduces encryption contents {data Data} Kc which newly received is the same as that of
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">drawing 9</A>
-
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014"
TARGET="tjitemdrw">drawing 12</A>
and
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017"
TARGET="tjitemdrw">drawing 15</A>
, and the flow chart shown in 16.

[0216]

Although the count length AC 1 of playback and the playback length AC 2 were explained as the count limit of playback, and playback length, respectively, as long as the count of playback adds a limit to the playback in a data playback terminal, it may perform limit [which] that the count length AC 1 of playback should just be control information which adds a limit to the treatment of a license with a recording device.

[0217]

Moreover, although the portable telephone 100 was explained as a Data Terminal Equipment which receives distribution of encryption contents data or a license, as long as it is especially unnecessary in a call function etc., it merely has the data communication facility which can perform reception of encryption contents data or a license and it can record the received data, you may be what kind of Data Terminal Equipment.

[0218]

Furthermore, although the portable telephone 100 is equipped with the function which reproduces contents data (music data), as long as it does not necessarily need a data regenerative function, but it merely has the data communication facility which can perform reception of encryption contents data or a license and it can record the received data, you may be what kind of Data Terminal Equipment.

[0219]

Furthermore, although it explained that encryption contents data or a license was recorded on the memory card which is a removable recording apparatus, it does not limit to a memory card.
And in the gestalt of operation, it is not necessary to be a removable recording device.

[0220]

According to the gestalt of operation of this invention, if the distribution demand of encryption contents data is inputted from a user, since the record situation of the memory card with which it was equipped will be searched and required encryption contents data, a license key, etc. will be received from a distribution server according to the record situation, encryption contents data, a license key, etc. overlap, and a portable telephone is not recorded on a memory card.
Moreover, it can prevent paying the useless tariff by overlapping and receiving a license to a distribution server.
Furthermore, it can prevent that useless time amount generates encryption contents data by overlapping and receiving.

[0221]

It should be thought that the gestalt of the operation indicated this time is [no] instantiation at points, and restrictive.
The range of this invention is shown by the above-mentioned not explanation but claim of the gestalt of operation, and it is meant that all modification in a claim, equal semantics, and within the limits is included.

<HR>DESCRIPTION OF DRAWINGS
<HR>[Brief Description of the Drawings]

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">[Drawing 1]</A>

It is the schematic diagram which explains a data distribution system notionally.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000004"
TARGET="tjitemdrw">[Drawing 2]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
, and information.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000005"
TARGET="tjitemdrw">[Drawing 3]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
, and information.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000006"
TARGET="tjitemdrw">[Drawing 4]</A>

It is drawing showing properties, such as data for the communication link in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
, and information.
.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000007"
TARGET="tjitemdrw">[Drawing 5]</A>

It is the outline block diagram showing the configuration of a license server.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000008"
TARGET="tjitemdrw">[Drawing 6]</A>

It is the block diagram showing the configuration of a portable telephone.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000009"
TARGET="tjitemdrw">[Drawing 7]</A>

It is the block diagram showing the configuration of a memory card.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000010"
TARGET="tjitemdrw">[Drawing 8]</A>

It is a conceptual diagram for explaining the record condition of a memory card.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000011"
TARGET="tjitemdrw">[Drawing 9]</A>

It is the 1st flow chart for explaining the distribution actuation in the data distribution system shown in
<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003"
TARGET="tjitemdrw">drawing 1</A>
.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000012"
TARGET="tjitemdrw">[Drawing 10]</A>

It is the 2nd flow chart for explaining the distribution actuation in the data distribution system shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003" TARGET="tjitemdrw">drawing 1</A>
.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000013" TARGET="tjitemdrw">[Drawing 11]</A>

It is the 3rd flow chart for explaining the distribution actuation in the data distribution system shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003" TARGET="tjitemdrw">drawing 1</A>
.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000014" TARGET="tjitemdrw">[Drawing 12]</A>

It is the 4th flow chart for explaining the distribution actuation in the data distribution system shown in
<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000003" TARGET="tjitemdrw">drawing 1</A>
.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000015" TARGET="tjitemdrw">[Drawing 13]</A>

It is drawing showing the condition of having displayed the contents menu transmitted to the portable telephone from the distribution server on the display of a portable telephone.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000016" TARGET="tjitemdrw">[Drawing 14]</A>

It is a data format in the memory of a memory card.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000017" TARGET="tjitemdrw">[Drawing 15]</A>

It is the 1st flow chart for explaining the playback actuation in a portable telephone.

<A HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B

%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000018"
TARGET="tjitemdrw">[Drawing 16]</A>

It is the 2nd flow chart for explaining the playback actuation in a portable telephone.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000019"
TARGET="tjitemdrw">[Drawing 17]</A>

It is drawing explaining the encryption contents data according to the record situation of a memory card, and the example of distribution of a license.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000020"
TARGET="tjitemdrw">[Drawing 18]</A>

It is a schematic diagram for explaining distribution of the encryption contents data using a computer notionally.

<A
HREF="http://www4.ipdl.ncipi.go.jp/cgi-bin/tran_web_cgi_ejje?u=http%3A%2F%2Fwww4.ipdl.ncipi.go.jp%2FTokujitu%2Ftjitemdrw.ipdl%3FN0000%3D237%26N0500%3D1E%5FN%2F%3B%3E%3B%3F6%3E7%3D8%2F%2F%2F%26N0001%3D12%26N0552%3D9%26N0553%3D000021"
TARGET="tjitemdrw">[Drawing 19]</A>

They are other schematic diagrams for explaining distribution of the encryption contents data using a computer notionally.

[Description of Notations]

10 License Server, 20 Distribution Carrier, 30 Distribution Server, 60 A contents menu, 100 A portable telephone, 110 Memory card, 130 A head telephone, 140 A computer, 141 Hard disk, 142, 1106, 1420 A controller, 143 External interface, 144 License ** A ** module, 145 Telecommunication cable, 302 An accounting database, a 304 information database, 306 CRL database, 307 A menu database, 308 Distribution record database, 310 The data-processing section, 312, 320, 1206, 1212, 1214, 1404, 1408 and 1412, the 1422 decode processing section, 313 An authentication key attaching part, 315 A distribution control section, 316, 1210, 1418 Session key generating section, 318, 326, 328, 1208, 1406, 1410 Cipher-processing section, 350 A communication device, 1102 An antenna, the 1104 transceiver sections, 1108 Key stroke section, 1110 A display, 1111 The shift section, 1112 Voice playback section, 1113 1218 A DA converter, 1114, 1201, 1220, 1224 Terminal, 1115 A microphone, 1116 An A-D converter, 1117 Voice coding section, 1200 1202 A memory interface, 1400 Authentication data-hold section, 1204 Kp1 attaching part, 1216 The music playback section, 1222 Switch, 1402 Kmc1 attaching part, 1414 A KPma attaching part, 1415 Memory, 1415A CRL field, 1415B A data area, 1416KPm1 attaching part, 1421 Km1 attaching part, 1423 An interface, 1424 Header, 1440 A license information attaching part, 1442, 1444, 1446 Change-over switch.

<HR></BODY></HTML>

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－91827
（P2002－91827A）
(43)公開日　平成14年３月29日(2002.3.29)

(51)Int.Cl.[7]		識別記号	FI		テーマコード*(参考)
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ 12/14	３２０Ｂ	５Ｂ０１７
	12/00	５３７	12/00	５３７Ｈ	５Ｂ０４９
	17/60	３０２	17/60	３０２Ｅ	５Ｂ０８２

審査請求　未請求　請求項の数14　ＯＬ　（全 31 頁）

(21)出願番号　特願2000－284862(P2000－284862)

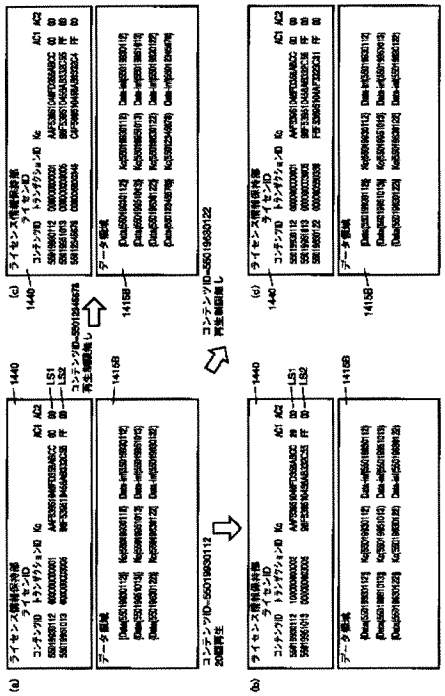
(22)出願日　平成12年９月20日(2000.9.20)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

Ｆターム(参考)　5B017 AA07 BA07 BB07 CA16
5B049 AA05 AA06 EE05 FF01 FF08 GG00
5B082 GA11

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　必要な暗号化コンテンツデータおよび／またはライセンス鍵等のみを配信サーバから受信する携帯端末装置を提供する。
【解決手段】　携帯電話機は、ユーザから暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの受信要求が入力されると、装着されたメモリカードにおけるコンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限情報ＡＣ１、再生期限、および暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ等の記録状況を検索する。そして、メモリカードのライセンス領域１４１５Ａ、データ領域１４１５Ｂに記録されていない暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス（コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限情報ＡＣ１、再生期限）だけを配信サーバから受信する。



【特許請求の範囲】
【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータおよび／または前記暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、前記暗号化コンテンツデータおよび／または前記ライセンスを記録するデータ端末装置であって、
前記暗号化コンテンツデータおよび前記ライセンスを記録するデータ記録部と、
外部との通信を行なう送受信部と、
前記データ記録部とのデータ授受を制御するインタフェースと、
指示を入力するためのキー操作部と、
制御部とを備え、
前記制御部は、前記キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータが前記データ記録装置に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生することができるライセンスの有無を検索し、
前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、および／または前記ライセンスが無いとき、前記暗号化コンテンツデータおよび／または前記ライセンスの配信を前記送受信部を介して配信サーバへ要求する、データ端末装置。
【請求項２】　前記制御部は、前記送受信部が前記配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項１に記載のデータ端末装置。
【請求項３】　前記受信要求する暗号化コンテンツデータの決定は、前記メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツＩＤが選択されることによって行なわれ、
前記制御部は、前記選択されたコンテンツＩＤに基づいて前記暗号化コンテンツデータおよび／または前記ライセンスの検索を行なう、請求項２に記載のデータ端末装置。
【請求項４】　前記制御部は、前記暗号化コンテンツデータの検索を行ない、前記暗号化コンテンツデータが前記データ記録部に記録されていないとき、前記暗号化コンテンツデータの配信を前記送受信部を介して前記配信サーバへ要求する、請求項１から請求項３のいずれか１項に記載のデータ端末装置。
【請求項５】　前記制御部は、前記暗号化コンテンツデータが前記データ記録装置に記録されているとき、前記ライセンスの検索を行なう、請求項４に記載のデータ端末装置。
【請求項６】　前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、
前記制御部は、受信要求された暗号化コンテンツデータが前記データ記録部に記録されており、前記ライセンス鍵および前記再生制限情報が前記データ記録部に記録されていないとき、前記ライセンスが無いと判断する、請求項１に記載のデータ端末装置。
【請求項７】　前記ライセンスは、少なくとも前記暗号化コンテンツデータを復号するためのライセンス鍵と、前記暗号化コンテンツデータの再生を制限する再生制限情報とから成り、
前記制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵が前記データ記録部に記録されており、前記暗号化コンテンツデータの再生が前記再生制限情報によって制限されているとき、前記ライセンスが無いと判断する、請求項１に記載のデータ端末装置。
【請求項８】　前記制御部は、前記キー操作部から入力された変更後の再生制限情報を前記ライセンスの購入条件として前記コンテンツＩＤとともに前記送受信部を介して前記配信サーバへ送信する、請求項７に記載のデータ端末装置。
【請求項９】　表示部をさらに備え、
前記制御部は、前記メニュー情報を前記表示部に表示し、ユーザが前記表示部に表示された前記メニュー情報に基づいて前記コンテンツＩＤを選択するための情報をキー操作部を介して入力することによって、前記コンテンツＩＤを取得する、請求項３に記載のデータ端末装置。
【請求項１０】　前記メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、
前記表示部は、前記移行情報を入力するための入力部を含み、
前記制御部は、前記入力部から前記移行情報が入力されると、前記移行情報に基づいて決定される他の画面を前記表示部に表示する、請求項９に記載のデータ端末装置。
【請求項１１】　前記制御部は、前記ライセンスの購入条件と、前記インタフェースを介して取得した前記データ記録部の認証データおよび前記コンテンツＩＤとを前記送受信部を介して前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証された場合のみ、前記ライセンスを受信する、請求項１から請求項１０のいずれか１項に記載のデータ端末装置。
【請求項１２】　前記ライセンスに従って前記暗号化コンテンツデータを再生するデータ再生部をさらに備え、
前記制御部は、前記キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報と前記暗号化コンテンツデ

ータとを前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項１から請求項１１のいずれか１項に記載のデータ端末装置。

【請求項１３】　前記バスに接続され、前記データ記録部に対する認証データを保持する認証データ保持部をさらに備え、

暗号化コンテンツデータの再生時、

前記制御部は、前記認証データが前記データ記録部において認証された場合のみ前記暗号化コンテンツデータに対する前記ライセンスのうち少なくとも前記データ再生部に必要な情報を前記データ記録部から前記インタフェースを介して受取り、その受取った暗号化コンテンツデータおよび前記必要な情報を前記データ再生部に与える、請求項１２に記載のデータ端末装置。

【請求項１４】　前記データ記録部は、着脱可能なデータ記録装置である、請求項１から請求項１３のいずれか１項に記載のデータ端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】

【発明が解決しようとする課題】しかし、暗号化コンテンツデータを配信サーバから受信するとき、携帯電話機は、暗号化コンテンツデータとともに暗号化コンテンツデータを復号するライセンス鍵、および暗号化コンテンツデータの再生回数、再生期限等を設定した購入条件を配信サーバから受信し、メモリカードに記録する。

【００１５】また、携帯電話機は、暗号化コンテンツデータを再生するとき、暗号化コンテンツデータの再生が受信した再生回数、再生期限等によって制限されないときに暗号化コンテンツデータを再生する。

【００１６】さらに、携帯電話機は、配信サーバ以外から暗号化コンテンツデータのみを受信し、メモリカードに記録する場合もある。

【００１７】したがって、暗号化コンテンツデータがメモリカードに記録されているが、ライセンス鍵がメモリカードに記録されていない場合、暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されているが、再生回数、再生期限等によって暗号化コンテンツデータの再生が制限される場合、および暗号化コンテンツデータおよびライセンス鍵がメモリカードに記録されていない場合等が想定される。

【００１８】かかる場合に、ユーザから暗号化コンテンツデータの配信要求がされた場合、直ちに配信サーバへ暗号化コンテンツデータおよびライセンス鍵等の配信を要求したのでは、同じ暗号化コンテンツデータおよびライセンス鍵を配信サーバから受信することになり、同じ暗号化コンテンツデータに対して料金を複数回支払うという問題が生じる。

【００１９】また、暗号化コンテンツデータを配信サーバから受信するために不要な時間を必要とするという問題もある。

【００２０】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、必要な暗号化コンテンツデータおよび／またはライセンス鍵等のみを配信サーバから受信するデータ端末装置を提供することである。

【００２１】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび／または暗号化コンテンツデータを再生するためのライセンスを配信サーバから受信して、暗号化コンテンツデータおよび／またはライセンスを記録するデータ端末装置であって、暗号化コンテンツデータおよびライセンスを記録するデータ記録部と、外部との通信を行なう送受信部と、データ記録部とのデータ授受を制御するインタフェースと、指示を入力するためのキー操作部と、制御部とを備え、制御部は、キー操作部を介して暗号化コンテンツデータの受信要求が入力されると、受信要求された暗号化コンテンツデータがデータ記録部に記録されているかを検索し、かつ、受信要求された暗号化コンテンツデータを再生するためのライセンスの有無を検索し、暗号化コンテンツデータがデータ記録部に記録されていないとき、および／またはライセンスが無いとき、暗号化コンテンツデータおよび／またはライセンスの配信を送受信部を介して配信サーバへ要求する。

【００２２】この発明によるデータ端末装置においては、ユーザから暗号化コンテンツデータの受信要求がキー操作部を介して入力されると、制御部は、受信要求がなされた暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索し、データ記録部に記録されていない暗号化コンテンツデータおよび／またはライセンスの配信を配信サーバへ要求する。つまり、データ端末装置は、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況に応じて必要な暗号化コンテンツデータおよびライセンスだけを配信サーバから受信し、かつ、データ記録部に記録する。

【００２３】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの重複記録を防止できる。

【００２４】また、この発明によれば、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。

【００２５】さらに、この発明によれば、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【００２６】好ましくは、データ端末装置の制御部は、送受信部が配信サーバから受信した暗号化コンテンツデータのメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に、暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００２７】データ端末装置は、配信サーバから受信したメニュー情報に基づいて、受信要求する暗号化コンテンツデータが決定された後に暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００２８】したがって、この発明によれば、受信要求された暗号化コンテンツデータおよびライセンスがデータ記録部に記録されているか否かを正確に判断できる。

【００２９】好ましくは、受信要求する暗号化コンテンツデータの決定は、メニュー情報に含まれた暗号化コンテンツデータを特定するためのコンテンツＩＤが選択されることによって行なわれ、制御部は、選択されたコンテンツＩＤに基づいて暗号化コンテンツデータおよび／またはライセンスの検索を行なう。

【００３０】ユーザは、暗号化コンテンツデータのコンテンツＩＤを特定することによって受信要求する暗号化コンテンツデータを選択する。そうすると、データ端末装置の制御部は、選択された暗号化コンテンツデータのコンテンツＩＤを抽出し、その抽出したコンテンツＩＤに基づいて、暗号化コンテンツデータおよび／またはライセンスがデータ記録部に記録されているか否かを検索する。

【００３１】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよび／またはライセンスの検索を正確に行なうことができる。

【００３２】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、暗号化コンテンツデータの配信を送受信部を介して配信サーバへ要求する。

【００３３】データ端末装置の制御部は、コンテンツＩＤを用いてデータ記録部における暗号化コンテンツデータの検索を行ない、暗号化コンテンツデータがデータ記録部に記録されていないとき、データ記録部におけるライセンスの検索を行なうわずに暗号化コンテンツデータおよびライセンスの配信を配信サーバへ要求する。

【００３４】したがって、この発明によれば、データ記録部における暗号化コンテンツデータおよびライセンスの記録状況を迅速に検索し、その記録状況に応じて必要な暗号化コンテンツデータおよびライセンスを配信サーバから受信できる。

【００３５】好ましくは、データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されているとき、ライセンスの検索を行なう。

【００３６】データ端末装置の制御部は、暗号化コンテンツデータがデータ記録部に記録されていないことを確認した後に、ライセンスの検索を行なう。

【００３７】したがって、この発明によれば、必要な検索のみを行なうことによって検索時間を短縮し、かつ、正確な検索を行なうことができる。

【００３８】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータがデータ記録装置に記録されており、ライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、ライセンスが無いと判断する。

【００３９】ライセンスを構成するライセンス鍵および再生制限情報がデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在したいと判断する。

【００４０】したがって、この発明によれば、データ記録部に暗号化コンテンツデータのみが記録されているとき、ライセンス鍵および再生制限情報を配信サーバから受信することができる。

【００４１】好ましくは、ライセンスは、少なくとも暗号化コンテンツデータを復号するためのライセンス鍵と、暗号化コンテンツデータの再生を制限する再生制限情報とから成り、制御部は、受信要求された暗号化コンテンツデータおよびその暗号化コンテンツデータを復号するためのライセンス鍵がデータ記録部に記録されており、暗号化コンテンツデータの再生が再生制限情報によって制限されているとき、ライセンスが無いと判断する。

【００４２】ライセンスを構成する再生制限情報のみがデータ記録部に記録されていないとき、データ端末装置の制御部は、受信要求された暗号化コンテンツデータのライセンスが存在しないと判断する。

【００４３】したがって、この発明によれば、再生制限情報のみがデータ記録部に記録されていないとき、再生制限情報を配信サーバから受信してライセンスを取得することができる。

【００４４】好ましくは、データ端末装置の制御部は、キー操作部から入力された変更後の再生制限情報をライセンスの購入条件としてコンテンツＩＤとともに送受信部を介して配信サーバへ送信する。

【００４５】データ端末装置の制御部は、再生制限情報のみを変更することによって暗号化コンテンツデータの購入条件が設定されると、コンテンツＩＤとともに設定された購入条件を配信サーバへ送信する。そして、データ端末装置は、再生制限情報を配信サーバから受信し、データ記録部に記録する。

【００４６】したがって、この発明によれば、ライセンスを購入して暗号化コンテンツデータを再生し、ライセンスが無くなった場合にも新たに再生制限情報だけを配信サーバから購入することによって暗号化コンテンツデータを再生することができる。

【００４７】好ましくは、データ端末装置は、表示部をさらに備え、制御部は、メニュー情報を表示部に表示し、ユーザが表示部に表示されたメニュー情報に基づいてコンテンツＩＤを選択するための情報をキー操作部を介して入力することによって、コンテンツＩＤを取得する。

【００４８】配信サーバから配信されたメニュー情報は、データ端末装置の表示部に表示される。そして、ユーザは表示部に表示されたメニュー情報を見て受信を希望する暗号化コンテンツデータのコンテンツＩＤを選択するための情報をキー操作部から入力する。そうすると制御部は、キー操作部を介して選択されたコンテンツＩＤを取得する。

【００４９】したがって、この発明によれば、ユーザは視覚情報に基づいて受信を希望する暗号化コンテンツデータを決定できる。また、この発明によれば、コンテンツＩＤを選択するための情報が入力されるので、制御部

は、選択されたコンテンツＩＤに基づいて、暗号化コンテンツデータおよび／またはライセンスの検索を迅速に行なうことができる。

【００５０】好ましくは、メニュー情報は、他の画面へ移行するための移行情報を含む複数の画面から構成され、表示部は、移行情報を入力するための入力部を含み、制御部は、入力部から移行情報が入力されると、移行情報に基づいて決定される他の画面を表示部に表示する。

【００５１】データ端末装置の表示部に表示されたメニュー情報に受信を希望する暗号化コンテンツデータが含まれていないとき、ユーザは移行情報を入力する、そうすると、データ端末装置の制御部は、次の画面に移行し、新たなメニュー情報を表示部に表示する。

【００５２】したがって、この発明によれば、多くの暗号化コンテンツデータの中から受信を希望する暗号化コンテンツデータを選択できる。

【００５３】好ましくは、データ端末装置の制御部は、ライセンスの購入条件と、インタフェースを介して取得したデータ記録部の認証データおよびコンテンツＩＤとを送受信部を介して配信サーバへ送信し、配信サーバにおいて認証データが認証された場合のみ、ライセンスを受信する。

【００５４】配信サーバがデータ記録部から送られてきた認証データを認証した場合のみ、データ端末装置はライセンスを受信する。

【００５５】したがって、この発明によれば、正規なデータ記録部にだけライセンスを与えることができる。その結果、暗号化コンテンツデータの保護を図ることができる。

【００５６】好ましくは、データ端末装置は、ライセンスに従って暗号化コンテンツデータを再生するデータ再生部をさらに備え、制御部は、キー操作部を介して暗号化コンテンツデータの再生要求が入力されると、暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報と暗号化コンテンツデータとをデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータおよび必要な情報をデータ再生部に与える。

【００５７】暗号化コンテンツデータの再生時、制御部は、ライセンスを構成する種々の情報のうち、再生に必要な情報だけをデータ記録部から取出し、暗号化コンテンツデータと、再生に必要な情報とをデータ再生部に与える。そして、データ再生部は、必要な情報によって暗号化コンテンツデータを復号および再生する。

【００５８】したがって、この発明によれば、再生に必要な情報によって暗号化コンテンツデータの再生を制限することができる。

【００５９】好ましくは、データ端末装置は、データ記録部に対する認証データを保持する認証データ保持部をさらに備え、暗号化コンテンツデータの再生時、制御部は、認証データがデータ記録部において認証された場合のみ暗号化コンテンツデータに対するライセンスのうち少なくともデータ再生部に必要な情報をデータ記録部からインタフェースを介して受取り、その受取った暗号化コンテンツデータをデータ再生部に与える。

【００６０】配信サーバから受信した暗号化コンテンツデータを再生するとき、データ記録部に対するデータ端末装置の正当性が確認された場合だけ、データ端末装置はデータ記録部から暗号化コンテンツデータを受取り、暗号化コンテンツデータを再生する。

【００６１】したがって、この発明によれば、正規なデータ端末装置だけが暗号化コンテンツデータを再生できる。その結果、暗号化コンテンツデータの不法なコピー等を防止して保護を図ることができる。

【００６２】好ましくは、データ記録部は、データ端末装置から着脱可能なデータ記録装置である。

【００６３】データ端末装置は、配信サーバから暗号化コンテンツデータおよびライセンスを受信すると、その受信した暗号化コンテンツデータおよびライセンスを着脱可能なデータ記録装置へに記録する。

【００６４】したがって、この発明によれば、複数のデータ記録装置に暗号化コンテンツデータおよび／またはライセンスを記録することができる。

【００６５】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００６６】図１は、本発明による携帯端末装置が再生の対象とする暗号化コンテンツデータをメモリカードへ配信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００６７】なお、以下では携帯電話機網を介してデジタル音楽データを各携帯電話ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【００６８】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、各携帯電話ユーザからの配信要求（配信リクエスト）をライセンスサーバに中継する。著作権の存在する音楽データを管理するライセンスサーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０で

ある携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてライセンスを与える。

【００６９】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

【００７０】図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生部（図示せず）に与える。

【００７１】さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００７２】以下では、このようなライセンスサーバ１０と配信キャリア２０と併せて、配信サーバ３０と総称することにする。

【００７３】また、このような配信サーバ３０から、各携帯電話機等にコンテンツデータを伝送する処理を「配信」と称することとする。

【００７４】このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ３０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００７５】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００７６】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信における暗号鍵を配信するための方式であり、さらに第２には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第３には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【００７７】本発明の実施の形態においては、特に、配信、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機とも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００７８】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００７９】まず、配信サーバ３０より配信されるデータについて説明する。Ｄａｔａは、音楽データ等のコンテンツデータである。コンテンツデータＤａｔａには、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ〔Ｄａｔａ〕Ｋｃがこの形式で配信サーバ３０より携帯電話ユーザに配布される。

【００８０】なお、以下においては、〔Ｙ〕Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００８１】さらに、配信サーバ３０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄａｔａ－ｉｎｆが配布される。また、配信サーバ３０からの暗号化コンテンツデータおよびライセンス鍵等の配信を特定するための管理コードであるトランザクションＩＤが配信サーバ３０と携帯電話機１００との間でやり取りされる。さらに、ライセンス情報としては、コンテンツデータＤａｔａを識別するためのコードであるコンテンツＩＤおよびライセンスの発行を特定できる管理コードであるライセンスＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）のアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１およびデータ再生端末における制御情報である再生期限ＡＣ２等が存在する。以後、ライセンス鍵Ｋｃとコンテンツ ＩＤとライセンスＩＤと再生回数期限ＡＣ１と再生期限ＡＣ２とを併せて、ライセンスと総称することとする。

【００８２】図３は、図１に示すデータ配信システムにおいて使用される認証および禁止クラスリストの運用のためのデータ、情報等の特性を説明する図である。

【００８３】本発明の実施の形態においては、記録装置（メモリカード）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【００８４】禁止クラスリスト関連情報には、ライセンスの配信、および再生が禁止される携帯電話機およびメモリカードのクラスをリストアップした禁止クラスリス

トデータＣＲＬが含まれる。

【００８５】禁止クラスリストデータＣＲＬは、配信サーバ３０内で管理されるとともに、メモリカード内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際の日時を基準として、携帯電話機から受取った禁止クラスリストの更新の有無を判断し、更新されていないとき、更新された禁止クラスリストを携帯電話機に配信する。また、禁止クラスリストの変更については、変更点のみを反映した差分データＣＲＬ＿ｄａｔを配信サーバ３０側より発生して、これに応じてメモリカード内の禁止クラスリストＣＲＬが書替えられる構成とするも可能である。また、禁止クラスリストのバージョンについては、ＣＲＬ＿ｖｅｒをメモリカード側より出力し、これを配信サーバ３０側で確認することによってバージョン管理を実行する。差分データＣＲＬ＿ｄａｔには新たなバージョンの情報も含まれる。

【００８６】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカード内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードへのライセンス鍵の供給を禁止する。このため、携帯電話機ではコンテンツデータの再生が、メモリカードではコンテンツデータの移動が行なえなくなる。

【００８７】このように、メモリカード内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード内における禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード内でタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【００８８】携帯電話機およびメモリカードには固有の公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉがそれぞれ設けられ、公開暗号鍵ＫＰｐｎおよびＫＰｍｃｉは携帯電話機に固有の秘密復号鍵Ｋｐｎおよびメモリカード固有の秘密復号鍵Ｋｍｃｉによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機の種類ごとおよびメモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【００８９】また、データ再生端末（携帯電話機）およびメモリカードのクラス証明書として、Ｃｒｔｆｎおよびｃｍｃｉがそれぞれ設けられる。これらのクラス証明書は、メモリカードおよびコンテンツ再生端末のクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【００９０】これらのメモリカードおよびコンテンツ再生端末固有の公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａおよび｛ＫＰｐｎ／／Ｃｒｔｆｎ｝ＫＰｍａの形式で、出荷時にメモリカードおよびデータ再生端末（携帯電話機）にそれぞれ記録される。後ほど詳細に説明するが、ＫＰｍａは配信システム全体で共通の公開認証鍵である。

【００９１】図４は、図１に示したデータ配信システムにおいて暗号化に関わる鍵の特性をまとめて説明する図である。

【００９２】メモリカード外とメモリカード間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ３０、携帯電話機１００、メモリカード１１０において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００９３】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、携帯電話機もしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００９４】これらのセッションキーＫｓ１～Ｋｓ３は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００９５】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍと、公開暗号鍵ＫＰｍで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵Ｋｍが存在する。

【００９６】図５は、図１に示したライセンスサーバ１０の構成を示す概略ブロック図である。

【００９７】ライセンスサーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、ライセンスＩＤ等の配信情報を保持するための情報データベース

３０４と、各携帯電話ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベースに保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、コンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００９８】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを復号するための公開認証鍵を保持する認証鍵保持部３１３と、メモリカードおよび携帯電話機から送られてきた認証のための認証データ｛ＫＰｍｃｉ／／Ｃｍｃｉ｝ＫＰｍａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰｍａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られた公開暗号鍵ＫＰｍｃｉを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００９９】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよび再生期限ＡＣ２を、復号処理部３２０によって得られたメモリカード固有の公開暗号鍵ＫＰｍによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１００】ライセンスサーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１０１】図６は、図１に示した携帯電話機１００の構成を説明するための概略ブロック図である。

【０１０２】携帯電話機１００は、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０２と、アンテナ１１０２からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ１１０２に与えるための送受信部１１０４と、携帯電話機１００の各部のデータ授受を行なうためのバスＢＳ２と、バスＢＳ２を介して携帯電話機１００の動作を制御するためのコントローラ１１０６とを含む。

【０１０３】携帯電話機１００は、さらに、外部からの指示を携帯電話機１００に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるためのディスプレイ１１１０と、通常の通話動作において、データベースＢＳ２を介して与えられる受信データに基づいて音声を再生するための音声再生部１１１２とを含む。

【０１０４】携帯電話機１００は、さらに、音声再生部１１１２の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１１１３と、ＤＡ変換器１１１３の出力を外部出力装置等へ出力するための端子１１１４とを含む。

【０１０５】携帯電話機１００は、さらに、通常の通話動作において、携帯電話機１００のユーザが話した音声信号を入力するマイク１１１５と、マイク１１１５からの音声信号をアナログ信号からディジタル信号に変換するＡＤ変換器１１１６と、ＡＤ変換器１１１６からのディジタル信号を所定の方式に従って符号化してバスＢＳ２へ与える音声符号化部１１１７とを含む。

【０１０６】携帯電話機１００は、さらに、配信サーバ３０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ２との間のデータの授受を制御するためのメモリインタフェース１２００とを含む。

【０１０７】携帯電話機１００は、さらに、携帯電話機の種類（クラス）ごとにそれぞれ設定される、公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｒｔｆ１を公開復号鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを保持する認証データ保持部１２０２を含む。ここで、携帯電話機（データ端末装置）１００のクラスｎは、ｎ＝１であるとする。

【０１０８】携帯電話機１００は、さらに、携帯電話機（コンテンツ再生回路）固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１２０４と、バスＢＳ２から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１２０６とを含む。

【０１０９】携帯電話機１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセ

ッションキー発生部１２１０と、発生されたセッションキーＫｓ３を復号処理部１２０６によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ２に出力する暗号化処理部１２０８とを含む。

【０１１０】携帯電話機１００は、さらに、バスＢＳ２上のデータをセッションキーＫｓ３によって復号して出力する復号処理部１２１２とを含む。

【０１１１】携帯電話機１００は、さらに、バスＢＳ２より暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受けて、復号処理部１２１２より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１２１４と、復号処理部１２１４の出力を受けてコンテンツデータを再生するための音楽再生部１２１６と、音楽再生部１２１６の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１２１８と、ＤＡ変換器１１１３とＤＡ変換器１２１８との出力を受けて、動作モードに応じて選択的に端子１１１４または端子１２２０から出力するためのスイッチ１２２２と、スイッチ１２２２の出力を受けて、ヘッドホーン１３０と接続するための接続端子１２２４とを含む。

【０１１２】なお、図６においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの配信および再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１１３】携帯電話機１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１１４】図７は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｃｉおよびＫｍｃｉが設けられ、メモリカードのクラス証明書Ｃｍｃｉが設けられるが、メモリカード１１０においては、これらは自然数ｉ＝１でそれぞれ表わされるものとする。

【０１１５】したがって、メモリカード１１０は、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａを保持する認証データ保持部１４００と、メモリカードの種類ごとに設定される固有の復号鍵であるＫｍｃ１を保持するＫｍｃ１保持部１４０２と、メモリカードごとに固有に設定される秘密復号鍵Ｋｍ１を保持するＫｍ１保持部１４２１と、Ｋｍ１によって復号可能な公開暗号鍵ＫＰｍ１を保持するＫＰｍ１保持部１４１６とを含む。認証データ保持部１４００は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵ＫＰｍｃ1およびクラス証明書Ｃｍｃ１を公開認証鍵ＫＰｍａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａとして保持する。

【０１１６】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１１７】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１２０１を介して授受するインタフェース１４２３と、インタフェース１４２３との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２３から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵Ｋｍｃ１をＫｍｃ１保持部１４０２から受けて、配信サーバ３０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４０４と、ＫＰｍａ保持部１４１４から認証鍵ＫＰｍａを受けて、バスＢＳ３に与えられるデータからＫＰｍａによる復号処理を実行して復号結果を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４４によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号化処理部１４０６とを含む。

【０１１８】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られる公開暗号鍵ＫＰｐｎもしくはＫＰｍｃｉによって暗号化してバスＢＳ３に送出する暗号化処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号し、復号結果をバスＢＳ４に送出する復号処理部１４１２とを含む。

【０１１９】メモリカード１１０は、さらに、バスＢＳ３上のデータを公開暗号鍵ＫＰｍ１と対をなすメモリカード１１０固有の秘密復号鍵Ｋｍ１によって復号するための復号処理部１４２２と、禁止クラスリストのバージョン更新のためのデータＣＲＬ＿ｄａｔによって逐次更新される禁止クラスリストデータＣＲＬをバスＢＳ４より受けて格納するとともに、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域１４１５Ａと、コンテンツＩＤを含むＨｅａｄｅｒ、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、および暗号化コンテンツデータの関連情報Ｄａｔａ－ｉｎｆを記録したデータ領域１４１５Ｂとから成る。

【０１２０】メモリカード１１０は、さらに、復号処理部１４２２によって得られるライセンスを保持するため

のライセンス情報保持部１４４０と、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１２１】ライセンス情報保持部１４４０は、Ｎ個（Ｎ：自然数）のバンクを有し、各ライセンスに対応するライセンスをバンクごとに保持する。

【０１２２】なお、図７において、実線で囲んだ領域は、メモリカード１１０内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊により、第三者に対してその領域内に存在する回路内のデータ等の読出を不能化するためのモジュールＴＲＭに組込まれているものとする。このようなモジュールは、一般にはタンパーレジスタンスモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ　Ｍｏｄｕｌｅ）である。

【０１２３】もちろん、メモリ１４１５も含めて、モジュールＴＲＭ内に組込まれる構成としてもよい。しかしながら、図７に示したような構成とすることで、メモリ１４１５中に保持されている再生に必要な再生情報は、いずれも暗号化されているデータであるため、第三者はこのメモリ１４１５中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ１４１５を設ける必要がないので、製造コストが低減されるという利点がある。

【０１２４】以降では、簡単化のためアクセス制御情報ＡＣ１は再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報ＡＣ２は再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報ＡＣ１および再生回路制御情報ＡＣ２を、それぞれ、再生回数制限ＡＣ１、再生期限ＡＣ２と称するものとする。

【０１２５】図８を参照して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃと、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２等から成るライセンスとが記録されたメモリカード１１０における各種の状態について説明する。なお、図８においては、再生回数制限ＡＣ１に制限がない場合を「ＦＦ」で表し、再生期限ＡＣ２に制限がない場合を「００」で表している。図８の（ａ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンスがメモリカード１１０に記録されており、新たに暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃとライセンスとを配信サーバ３０から受信する場合を示す。また、図８の（ｂ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃが存在し、一部、再生回数制限ＡＣ１によって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの再生が制限されている場合を示す。さらに、図８の（ｃ）は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃとライセンスとが記録されており、一部の暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを再生するライセンスが記録されていない場合を示す。

【０１２６】図８の（ａ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３，５５０１９６３０１２２によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５，Ｆ６Ｆ５３６９５１０４ＡＦ３３２３Ｃ３１が記録されている。また、コンテンツＩＤ：５５０１９９５１０１３，５５０１９６３０１２２によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であるが、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータの再生回数制限ＡＣ１は２０回、再生期限ＡＣ２は無制限である。したがって、データ領域１４１５Ｂに記録された３つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃに対するライセンスはライセンス情報保持部１４４０に記録されている。

【０１２７】図８の（ｂ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５が記録されている。また、コンテンツＩＤ：５５０１９９５１０１３によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であるが、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータの再生回数制限ＡＣ１は０回、再生期限ＡＣ２は無制限である。したがって、データ領域１４１５Ｂに記録された２つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのうち、１つの暗号化コンテンツデータはライセンスがライセンス情報保持部１４４０に記録されていない。

【０１２８】図８の（ｃ）を参照して、コンテンツＩＤ：５５０１９９３０１１２，５５０１９９５１０１３によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、その暗号化コンテンツデータを復号するためのライセンス鍵：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ，９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５が記録されている。また、コンテ

ンツＩＤ：５５０１９９５１０１３によって特定される暗号化コンテンツデータは再生回数制限ＡＣ１および再生期限ＡＣ２が無制限であり、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータの再生回数制限ＡＣ１は２０回、再生期限ＡＣ２は無制限である。さらに、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）はデータ領域１４１５Ｂに記録されているが、その暗号化コンテンツデータを再生するためのライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２から成るライセンスはライセンス情報保持部１４４０に記録されていない。したがって、データ領域１４１５Ｂに記録された３つの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのうち、１つの暗号化コンテンツデータに対するライセンスが存在しない。

【０１２９】図８を参照して説明したように、メモリカード１１０には、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２が記録されているか否かによって各種の状態が存在する。

【０１３０】次に、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等が各種の状態で記録されたメモリカード１１０が携帯電話機１００に装着され、携帯電話機１００のユーザから暗号化コンテンツデータの受信要求がされた場合の動作について説明する。

【０１３１】図９～図１２は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０１３２】図９を参照して、携帯電話機１００のユーザからキー操作部１１０８を介してコンテンツデータの配信要求がなされると、携帯電話機１００は、コンテンツメニューの送信要求を配信サーバ３０へ送信する（ステップＳ７０）。配信サーバ３０の配信制御部３１５は、通信装置３５０およびバスＢＳ１を介してコンテンツメニューの送信要求を受信すると（ステップＳ７２）、メニューデータベース３０７からバスＢＳ１を介してコンテンツメニューを読出し、その読出したコンテンツメニューをバスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ７４）。携帯電話機１１０は、送受信部１１０４によってコンテンツメニューを受信し、コントローラ１１０６は、コンテンツメニューを表示部１１１０に表示する（ステップＳ７６）。

【０１３３】そうすると、携帯電話機１００の表示部１１１０には、図１３に示すコンテンツメニュー６０が表示される。ユーザは、コンテンツメニュー６０の番号００１，００２，００３，・・・を選択することによって配信を希望する暗号化コンテンツデータを選択する。表示部１１１０には、別の画面に移行するための移行部１１１１が設けられている。ユーザは、表示部１１１０に表示されたコンテンツメニュー６０中に希望する暗号化コンテンツデータが表示されていないとき、移行部１１１１をクリックする。移行部１１１１には、別の画面へ移行するためのアドレスが含まれている。

【０１３４】携帯電話機１００のコントローラ１１０６は、コンテンツが選択された否かを判断し（ステップＳ７８）、移行部１１１１がクリックされると、コントローラ１１０６は、移行部１１１１に含まれるアドレスを送受信部１１０４を介して配信サーバ３０へ送信し、別の画面を送信するように要求する。そして、ステップＳ７０～Ｓ７８が繰返される。つまり、コンテンツメニューは、コンテンツメニュー６０から成る複数個の画面が階層的に配列されて構成されており、各画面は、ジャンルの異なる暗号化コンテンツデータ、同じジャンルであるが、他の暗号化コンテンツデータ等から成るコンテンツメニューによって構成されている。

【０１３５】そして、配信サーバ３０から複数の画面によって送られてきたコンテンツメニューに、希望する暗号化コンテンツデータが含まれていないとき、配信動作はステップＳ１７０へ移行し、配信動作は終了する。

【０１３６】コンテンツメニュー６０は、暗号化コンテンツデータを特定するためのコンテンツＩＤを含んでおり、ステップＳ７８において暗号化コンテンツデータが選択されたとき、コンテンツメニューから選択された暗号化コンテンツデータのコンテンツＩＤが抽出される（ステップＳ８０）。

【０１３７】そして、キー操作部１１０８を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ８２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータの再生回数制限ＡＣ１、および再生期限ＡＣ２を設定して購入条件ＡＣが入力される。

【０１３８】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０６は、選択された暗号化コンテンツデータに対するコンテンツＩＤと同じコンテンツＩＤを有する暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されていないかを検索する（ステップＳ８４）。この場合、コントローラ１１０６は、選択された暗号化コンテンツデータに対応するコンテンツＩＤをメモリインタフェース１２００を介してメモリカード１１０へ送信する。メモリカード１１０のコントローラ１４２０は、インタフェース１４２３およびバスＢＳ３を介して携帯電話機１００からコンテンツＩＤを受取り、その受取ったコンテンツＩＤがメモリ１４１５のＨｅａｄｅｒ１４２４に含まれるコンテンツＩＤと一致するか否かによって、ユーザがコンテン

ツメニューから選択した暗号化コンテンツデータがメモリカード１１０に記録されているか否かを検索する。

【０１３９】この場合、メモリカード１１０のメモリ１４１５に記録されたＨｅａｄｅｒ、Ｄａｔａ－ｉｎｆ、および｛Ｄａｔａ｝Ｋｃを図１４に示すように１つのデータ列としてハッシュ関数などを用いた署名データを併せて取扱うようにすれば、コンテンツＩＤの改組を防止することができる。署名の確認は、コンテンツＩＤの検査時に対応したものに関しても行なえば良い。

【０１４０】そして、コントローラ１１０６は、選択した暗号化コンテンツデータがメモリカード１１０に記録されているか否かを判断し（ステップＳ８６）、暗号化コンテンツデータがメモリカード１１０に記録されていないとき、データを配信サーバ３０から取得するためのフラグ”Ｙｅｓ”を立てる（ステップＳ８８）。暗号化コンテンツデータがメモリカード１１０に記録されているとき、ライセンスの確認が行なわれる（ステップＳ９０）。つまり、図８を参照して説明したようにライセンス鍵Ｋｃがメモリカード１１０に記録されているか、再生回数制限ＡＣ１および再生期限ＡＣ２によって暗号化コンテンツデータの再生が制限されていないかによってライセンスの確認が行なわれる。ライセンスが存在しないときはステップＳ９４へ移行する。ライセンスが存在し、暗号化コンテンツデータが再生できる場合、コントローラ１１０６は、「ライセンス単体購入？」を表示部１１１０に表示し、ライセンスだけを単体で購入するか否かの意思を確信する（ステップＳ９２）。コントローラ１１０６は、ライセンスだけを購入しない旨の指示がキー操作部１１０８から入力されると、ステップＳ１７０へ移行し、暗号化コンテンツデータの配信動作は終了する。コントローラ１１０６は、ライセンスだけを単体で購入する旨の指示がキー操作部１１０８から入力されると、データを配信サーバ３０から取得しないフラグ”Ｎｏ”を立てる（ステップＳ９４）。

【０１４１】次に、図１０を参照して、携帯電話機１００は、ユーザが暗号化コンテンツデータを選択することによって抽出したコンテンツＩＤ（ステップＳ８０参照）の指定による配信リクエストがなされる（ステップＳ１００）。

【０１４２】メモリカード１１０においては、この配信リクエストに応じて、認証データ保持部１４００より認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａが出力される（ステップＳ１０２）。

【０１４３】携帯電話機１００は、メモリカード１１０からの認証のための認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣとを配信サーバ３０に対して送信する（ステップＳ１０４）。

【０１４４】配信サーバ３０では、携帯電話機１００からコンテンツＩＤ、認証データ｛ＫＰｍｃ１／／Ｃｍｃ１｝ＫＰｍａ、ライセンス購入条件のデータＡＣを受信し（ステップＳ１０６）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰｍａで復号処理を実行する（ステップＳ１０８）。

【０１４５】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからの公開暗号鍵ＫＰｍｃ１と証明書Ｃｍｃ１を保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１０）。正当な認証データであると判断された場合、配信制御部３１５は、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を承認し、受理する。そして、次の処理（ステップＳ１１２）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍｃ１および証明書Ｃｍｃ１を受理しないで処理を終了する（ステップＳ１７０）。

【０１４６】認証の結果、正規の機器であることが認識されると、配信制御部３１５は、次に、メモリカード１１０のクラス証明書Ｃｍｃ１が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１７０）。

【０１４７】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１２）。

【０１４８】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ３０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１３）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応する公開暗号鍵ＫＰｍｃ１によって、暗号化処理部３１８によって暗号化される（ステップＳ１１４）。

【０１４９】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１１６）。

【０１５０】携帯電話機１００が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍｃ１を受信すると（ステップＳ１１８）、メモリカード１１０においては、メモリインタフェース１２００を介して、バスＢＳ３に与えられた受信データを、復号処理部１４０４が、保持部１４０２に

保持されるメモリカード１１０固有の秘密復号鍵Ｋｍｃ１により復号処理することにより、セッションキーＫｓ１を復号し抽出する（ステップＳ１２０）。

【０１５１】コントローラ１４２０は、配信サーバ３０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対して、メモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。

【０１５２】また、配信セッションにおいては、コントローラ１４２０は、メモリカード１１０内のメモリ１４１５に記録されている禁止クラスリストのデータＣＲＬ＿ｄａｔをメモリ１４１５から抽出してバスＢＳ４に出力する。

【０１５３】暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４０４より与えられるセッションキーＫｓ１によって、切換スイッチ１４４４および１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、公開暗号鍵ＫＰｍ１および禁止クラスリストのデータＣＲＬ＿ｄａｔを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１２２）。

【０１５４】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｖｅｒ｝Ｋｓ１は、バスＢＳ３からインタフェース１４２３、端子１２０１およびメモリインタフェース１２００を介して携帯電話機１００に出力され、携帯電話機１００から配信サーバ３０に送信される（ステップＳ１２４）。

【０１５５】配信サーバ３０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、メモリカード１１０固有の公開暗号鍵ＫＰｍ１およびメモリカード１１０における禁止クラスリストのデータＣＲＬ＿ｄａｔを受理する（ステップＳ１２６）。

【０１５６】配信制御部３１５は、ステップＳ１０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、ライセンスＩＤ、アクセス制限情報ＡＣ１および再生期限ＡＣ２を生成する（ステップＳ１２８）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ１３０）。

【０１５７】配信制御部３１５は、生成したライセンス、すなわち、ライセンス鍵Ｋｃ、再生期限ＡＣ２、ライセンスＩＤ、コンテンツＩＤ、およびアクセス制限情報ＡＣ１を暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたメモリカード１１０固有の公開暗号鍵ＫＰｍ１によってライセンスを暗号化する（ステップＳ１３２）図１１を参照して、配信サーバ３０において、メモリカード１１０から送信された禁止クラスリストのデータＣＲＬ＿ｄａｔが最新か否かが判断され、データＣＲＬ＿ｄａｔが最新と判断されたとき、ステップＳ１３４へ移行する。また、データＣＲＬ＿ｄａｔが最新でないときはステップＳ１３７へ移行する（ステップＳ１３３）。

【０１５８】データＣＲＬ＿ｄａｔが最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１をメモリカード１１０において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を通信装置３５０を介して携帯電話機１００へ送信する（ステップＳ１３４）。

【０１５９】そして、携帯電話機１００は、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を受信し（ステップＳ１３５）、バスＢＳ２およびメモリインタフェース１２００を介してメモリカード１１０へ送信する。メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１｝Ｋｓ２を端子１２０１およびインタフェース１４２３を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１を受理する（ステップＳ１３６）。その後、ステップＳ１４６へ移行する。

【０１６０】一方、配信サーバ３０において、ＣＲＬ＿ｄａｔが最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストのデータＣＲＬ＿ｄａｔを取得する（ステップＳ１３７）。

【０１６１】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの最新データＣＲＬ＿ｄａｔとを受けて、メモリカード１１０において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データは、バスＢＳ１および通信装置３５０を介して携帯電話機１００に送信される（ステップＳ１３８）。

【０１６２】このように、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行な

うことができ、データ配信システムのセキュリティを向上させることができる。

【０１６３】携帯電話機１００は、送信された暗号化データ｛｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１／／ＣＲＬ＿ｄａｔ｝Ｋｓ２を受信し（ステップＳ１４０）、メモリインタフェース１２００を介してメモリカード１１０へ出力する。メモリカード１１０においては、端子１２０１およびインタフェース１４２３を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３の受信データを復号しバスＢＳ４に出力する（ステップＳ１４２）。

【０１６４】この段階で、バスＢＳ４には、Ｋｍ１保持部１４２１に保持される秘密復号鍵Ｋｍ１で復号可能な暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１と、ＣＲＬ＿ｄａｔとが出力される（ステップＳ１４２）。コントローラ１４２０の指示によって受理した最新の禁止クラスリストＣＲＬ＿ｄａｔによってメモリ１４１５内の禁止クラスリストＣＲＬが書き換えられる（ステップＳ１４４）。

【０１６５】ステップＳ１３４，Ｓ１３５，Ｓ１３６は、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが最新の場合のライセンス鍵Ｋｃ等のメモリカード１１０への配信動作であり、ステップＳ１３７，Ｓ１３８，Ｓ１４０，Ｓ１４２，Ｓ１４４は、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが最新でない場合のライセンス鍵Ｋｃ等のメモリカード１１０への配信動作である。このように、メモリカード１１０から送られてきた禁止クラスリストＣＲＬ＿ｄａｔが更新されているか否かを、逐一、確認し、更新されていないとき、最新の禁止クラスリストＣＲＬ＿ｄａｔをＣＲＬデータベース３０６から取得し、メモリカード１１０に配信することによって、ライセンスの破られたメモリカードへの暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信を防止し、かつ、ライセンスの破られた携帯電話機による暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの再生を防止できる。

【０１６６】ステップＳ１３６またはステップＳ１４４の後、コントローラ１４２０の指示によって、暗号化ライセンス｛Ｋｃ／／ＡＣ２／／ライセンスＩＤ／／コンテンツＩＤ／／ＡＣ１｝Ｋｍ１は、復号処理部１４２２において、秘密復号鍵Ｋｍ１によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、再生回数制限ＡＣ１および再生期限ＡＣ２）が受理される（ステップＳ１４８）。

【０１６７】コントローラ１４２０は、ライセンスをライセンス情報保持部１４４０に記録する（ステップＳ１５０）。

【０１６８】図１２を参照して、携帯電話機１００のコントローラ１１０６は、ステップＳ８８およびステップＳ９４において立てたフラグを参照し、配信サーバ３０から暗号化コンテンツデータを取得するか否かを判断する。そして、暗号化コンテンツデータを配信サーバ３０から取得しないとき、ステップＳ１６４へ移行し、暗号化コンテンツデータを配信サーバ３０から取得するとき、ステップＳ１５４へ移行する。

【０１６９】暗号化コンテンツデータを配信サーバ３０から取得するとき、携帯電話機１００は、配信サーバ３０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ３０へ送信する（ステップ１５４）。

【０１７０】配信サーバ３０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１５６）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１５８）。

【０１７１】携帯電話機１００は、｛Ｄａｔａ｝Ｋｃ／／Ｄａｔａ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆを受理する（ステップＳ１６０）。暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆは、メモリインタフェース１２００、端子１２０１、およびインタフェース１４２３を介してメモリカード１１０のバスＢＳ３に伝達される。メモリカード１１０においては、受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよび付加情報Ｄａｔａ－ｉｎｆがそのままメモリ１４１５に記録される（ステップＳ１６２）。

【０１７２】そして、ステップＳ１５２において暗号化コンテンツデータを配信サーバ３０から受信しないと判断されたときも含め、メモリカード１１０から配信サーバ３０へは、トランザクションＩＤ／／配信受理の通知が送信され（ステップＳ１６４）、配信サーバ３０でトランザクションＩＤ／／配信受理を受信すると（ステップＳ１６６）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１６８）、全体の処理が終了する（ステップＳ１７０）。

【０１７３】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍｃ１とともに暗号化して送信できた公開暗号鍵Ｋｐ１およびＫｍｃ１が有効であることを確認した上で、それぞれのクラス証明書Ｃｍｃ１が禁止クラスリスト、すなわち、公開暗号鍵Ｋｐ１およびＫｍｃ１による暗号化が破られたクラス証明書リストに記

載されていないメモリカードからの配信要求に対してのみコンテンツデータを配信することができ、不正なメモリカードへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０１７４】また、配信サーバ３０への暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求時にメモリカード１１０における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、ライセンス鍵Ｋｃ、および再生回数制限ＡＣ１等の記録状況に応じて、必要な配信だけを配信サーバ３０に要求することができる。その結果、無駄な配信を防止することができる。

【０１７５】次に、図１５および図１６を参照してメモリカード１１０に配信されたコンテンツデータの携帯電話機１００における再生動作について説明する。図１５を参照して、再生動作の開始とともに、携帯電話機１００のユーザからキー操作部１１０８を介して再生指示が携帯電話機１００にインプットされる（ステップＳ２００）。そうすると、コントローラ１１０６は、バスＢＳ２を介して認証データ保持部１２０２から認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを読出し、メモリインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを入力する（ステップＳ２０１）。

【０１７６】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを受理する（ステップＳ２０２）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａを、ＫＰｍａ保持部１４１４に保持された公開認証鍵ＫＰｍａによって復号し（ステップＳ２０３）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｒｔｆ１｝ＫＰｍａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ２０４）。復号できなかった場合、コントローラ１４２０は認証データ不受理の出力をデータＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。認証データが復号できた場合、コントローラ１４２０は、取得した証明書Ｃｒｔｆ１がメモリ１４１５から読出した禁止クラスリストデータに含まれるか否かを判断する（ステップＳ２０５）。この場合、証明書Ｃｒｔｆ１にはＩＤが付与されており、コントローラ１４２０は、受理した証明書Ｃｒｔｆ１のＩＤが禁止クラスリストデータの中に存在するか否かを判別する。証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれると判断されると、コントローラ１４２０は認証データ不受理の出力をデータＢＳ３および端子１２０１を介して携帯電話機１００のメモリインタフェース１２００へ出力する（ステップＳ２０６）。

【０１７７】ステップＳ２０４において認証データが公開認証鍵ＫＰｍａで復号できなかったとき、およびステップＳ２０５において受理した証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれているとき、認証データ不受理の出力がなされる。そして、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して認証データ不受理の出力を受けると、認証データ不受理のデータをディスプレイ１１１０に表示する（ステップＳ２０７）。

【０１７８】ステップＳ２０５において、証明書Ｃｒｔｆ１が禁止クラスリストデータに含まれていないと判断されると、図１６を参照して、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ２０８）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ２０９）。そうすると、コントローラ１４２０は、端子１２０１を介してメモリインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力し、携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１２０４は、秘密復号鍵Ｋｐ１を復号処理部１２０６へ出力する。

【０１７９】復号処理部１２０６は、Ｋｐ１保持部１２０４から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１２０８へ出力する（ステップＳ２１０）。そうすると、セッションキー発生部１２１０は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１２０８へ出力する（ステップＳ２１１）。暗号処理部１２０８は、セッションキー発生部１２１０からのセッションキーＫｓ３を復号処理部１２０６からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ２およびメモリインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ２１２）。

【０１８０】メモリカード１１０の復号処理部１４１２は、端子１２０１、インタフェース１４２３、およびバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力し、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を取得する（ステップＳ２１３）。

【０１８１】セッションキーＫｓ３の受理に応じて、コントローラ１４２０は、ライセンス情報保持部１４４０内の対応するアクセス制限情報ＡＣ１を確認する（ステップＳ２１４）。

【０１８２】ステップＳ２１４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣ１を確認することにより、既に再生不可の状態である場合には再生動作を終了し、再生回数制限に制限がある場合にはアクセス制限情報ＡＣ１のデータを更新し再生可能回数を更新した後に次のステップに進む（ステップＳ２１５）。一方、アクセス制限情報ＡＣ１によって再生回数制限が制限されていない場合においては、ステップＳ２１５はスキップされ、再生回数制限ＡＣ１は更新されることなく処理が次のステップ（ステップＳ２１６）に進行される。

【０１８３】また、ライセンス情報保持部１４４０内にリクエスト曲の当該コンテンツＩＤが存在しない場合においても、再生不可の状態にあると判断して、再生動作を終了する。

【０１８４】ステップＳ２１４において、当該再生動作において再生が可能であると判断された場合には、ライセンス情報保持部１４４０に記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生期限ＡＣ２がバスＢＳ４上に出力される（ステップＳ２１６）。

【０１８５】得られたライセンス鍵Ｋｃと再生期限ＡＣ２は、切換スイッチ１４４４の接点Ｐｄを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｄを介して復号処理部１４１２より受けたセッションキーＫｓ３によってバスＢＳ４から受けたライセンス鍵Ｋｃと再生期限ＡＣ２とを暗号化し、｛Ｋｃ／／ＡＣ２｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ２１７）。

【０１８６】バスＢＳ３に出力された暗号化データは、インタフェース１４２３、端子１２０２、およびメモリインタフェース１２００を介して携帯電話機１００に送出される。

【０１８７】携帯電話機１００においては、メモリインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣ２｝Ｋｓ３を復号処理部１２１２によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣ２を受理する（ステップＳ２１８）。復号処理部１２１２は、ライセンス鍵Ｋｃを復号処理部１２１４に伝達し、再生期限ＡＣ２をバスＢＳ２に出力する。

【０１８８】コントローラ１１０６は、バスＢＳ２を介して、再生期限ＡＣ２を受理して再生の可否の確認を行なう（ステップＳ２１９）。

【０１８９】ステップＳ２１９においては、再生期限ＡＣ２によって再生不可と判断される場合には、再生動作は終了される。

【０１９０】ステップＳ２１９において再生可能と判断された場合、コントローラ１１０６は、メモリインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ３および端子１２０１を介してメモリインタフェース１２００へ出力する（ステップＳ２２０）。

【０１９１】携帯電話機１００のコントローラ１１０６は、メモリインタフェース１２００を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１４へ与える。そして、復号処理部１２１４は、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号処理部１２１２から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ２２１）。

【０１９２】そして、復号されたコンテンツデータＤａｔａは音楽再生部１２１６へ出力され、音楽再生部１２１６は、コンテンツデータを再生し、ＤＡ変換器１２１８はディジタル信号をアナログ信号に変換して端子１２２０へ出力する。そして、スイッチ１２２２は端子１２２０を選択して音楽データは端子１２２４を介してヘッドホーン１３０へ出力されて再生される（ステップＳ２２２）。これによって再生動作が終了する。

【０１９３】図１７を参照して、メモリカード１１０における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等の記録状況に応じた暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃ等の配信の例について説明する。図１７の（ａ）を参照して、メモリカード１１０のデータ領域１４１５Ｂには、暗号化コンテンツデータ：｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）、｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）と、それぞれの関連情報Ｄａｔａ－ｉｎｆとが記録されている。また、ライセンス領域１４１５Ａには、コンテンツＩＤ：５５０１９９３０１１２、トランザクションＩＤ：０００００００００００１、ライセンス鍵Ｋｃ：ＡＡＦ５３９５１０４６ＦＤ３５６ＡＢＣＣ、再生回数制限ＡＣ１：００、再生期限ＡＣ２：００のライセンスＬＳ１と、コンテンツＩＤ：５５０１９９５１０１３、トランザクションＩＤ：０００００００３００５、ライセンス鍵Ｋｃ：９６Ｆ５３９５１０４５６ＡＢ３３２Ｃ５５、再生回数制限ＡＣ１：ＦＦ、再生期限ＡＣ２：００のライセンスＬＳ２とが記録されている。そして、ライセンスＬＳ１については、再生回数制限ＡＣ１は「００」であるので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生できない、すなわち、ライセンスがない状態を示している。また、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２

２）について、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２が記録されておらず、ライセンスがない状態を示している。つまり、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９５１０１３）｝Ｋｃ（５５０１９９５１０１３）に対するライセンスＬＳ２だけが存在し、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）、および｛Ｄａｔａ（５５０１９６３０１２２｝Ｋｃ（５５０１９６３０１２２）に対するライセンスが存在しない状況である。

【０１９４】図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１９９３０１１２が抽出される（ステップＳ８０）。そして、ステップＳ８２において、「２０」回まで再生可能とするライセンスの購入条件ＡＣが入力される。そして、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。

【０１９５】この場合、コンテンツＩＤ：５５０１９９３０１１２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、メモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）として記録されているので、図９のステップＳ８６を介してステップＳ９０へ移行する。そして、ステップＳ９０において、ライセンスによって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）が再生可能か否かが判断される。この場合、再生回数制限ＡＣ１が「００」であるので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生することができない。したがって、ステップＳ９０からステップＳ９４へ移行する。そして、ステップＳ９４においてデータ取得＝”Ｎｏ”のフラグが立てられた後、ステップＳ１００～ステップＳ１７０によって再生回数制限ＡＣ１を「２０」回とするライセンスだけが配信サーバ３０からメモリカード１１０に配信される。そして、図１７の（ｂ）に示すようにライセンスＬＳ１の再生回数制限ＡＣ１が「２０」と変更される。これによって、ライセンスＬＳ１によって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９９３０１１２）｝Ｋｃ（５５０１９９３０１１２）を再生することができる。

【０１９６】また、図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１２３４５６７８が抽出される（ステップＳ８０）。その後、ライセンスの購入条件ＡＣとして、ＡＣ１：ＦＦ、ＡＣ２：００の再生制限なしが入力される（ステップＳ８２）。そして、コンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。この場合、コンテンツＩＤ：５５０１２３４５６７８によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃはメモリカード１１０に記録されていないので、ステップＳ８６からステップＳ８８へ移行し、ステップＳ８８においてデータ取得＝”Ｙｅｓ”のフラグが立てられる。

【０１９７】その後、ステップＳ１００～ステップＳ１７０が実行され、メモリカード１１０にコンテンツＩＤ：５５０１２３４５６７８、トランザクションＩＤ：０００００５５００３４５、ライセンス鍵Ｋｃ：Ｃ６Ｆ５６９５１０４５６ＡＢ３３３Ｃ４、再生回数制限ＡＣ１：ＦＦ、再生期限ＡＣ２：００、暗号化コンテンツデータ：｛Ｄａｔａ（５５０１２３４５６７８）｝Ｋｃ（５５０１２３４５６７８）、および関連情報ＤａｔａＤ－ｉｎｆ（５５０１２３４５６７８）が配信され、かつ、記録される。これによって、メモリカード１１０は、図１７の（ｃ）に示す状態になり、ユーザが配信要求を行なった暗号化コンテンツデータ｛Ｄａｔａ（５５０１２３４５６７８）｝Ｋｃ（５５０１２３４５６７８）の再生が可能となる。

【０１９８】さらに、図１７の（ａ）に示すメモリカード１１０の状況において、携帯電話機１００のユーザからコンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求がキー操作部１１０８を介して入力されると、図９のステップＳ７０～Ｓ７８が行なわれ、コンテンツＩＤ：５５０１９６３０１２２が抽出される（ステップＳ８０）。その後、ライセンスの購入条件ＡＣとして、ＡＣ１：ＦＦ、ＡＣ２：００の再生制限なしが入力される（ステップＳ８２）。そして、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃがメモリカード１１０に記録されているか否かが検索される（ステップＳ８４）。この場合、コンテンツＩＤ：５５０１９６３０１２２によって特定される暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃはメモリカード１１０に記録されているので、ステップＳ８６からステップＳ９０へ移行する。そして、ステップＳ９０において、ライセンスによって暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）が再生可能か否かが判断さ

れる。この場合、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣのいずれもメモリカード１１０に記録されていないので、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）を再生することができない。したがって、ステップＳ９０からステップＳ９４へ移行する。

【０１９９】そして、ステップＳ９４においてデータ取得＝”Ｎｏ”のフラグが立てられた後、ステップＳ１００～ステップＳ１７０によって再生制限なしとするライセンスだけが配信サーバ３０からメモリカード１１０に配信される。そして、図１７の（ｄ）に示すようにコンテンツＩＤ：５５０１９６３０１２２、トランザクションＩＤ：０００００５５０３３９、ライセンス鍵Ｋｃ：Ｆ６Ｆ５３６９５１０４ＡＦ３３２３Ｃ３１、再生回数制限ＡＣ１：ＦＦ、および再生期限：００がメモリカード１１０のライセンス領域１４１５Ａに記録される。これによって、暗号化コンテンツデータ｛Ｄａｔａ（５５０１９６３０１２２）｝Ｋｃ（５５０１９６３０１２２）を再生することができる。

【０２００】上述したように、携帯電話機１００のユーザは、メモリカード１１０における暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃ、およびライセンス鍵Ｋｃ等の記録状況に応じて、携帯電話機１００を用いて配信サーバ３０から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃおよびライセンス鍵Ｋｃ等をメモリカード１１０に受信し、ライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを復号し、かつ、再生することができる。

【０２０１】上記においては、携帯電話機１００のユーザが暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信要求を行なうとき、メモリカード１１０に記録されている暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、配信サーバ３０から受信した暗号化コンテンツデータであるとして説明したが、本発明においては、かかる場合に限らず、配信サーバ３０以外から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃだけを受信し、メモリカード１１０に記録した場合も含まれる。

【０２０２】図１８および図１９を参照して、配信サーバ３０以外の装置から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを受信し、その暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０に記録する場合について説明する。

【０２０３】図１８を参照して、コンピュータ１４０を用いた暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの配信について説明する。携帯電話機１００にはメモリカード１１０が着脱可能であり、音楽を再生するためのヘッドホン１３０が接続されている。そして、携帯電話機１００は、通信ケーブル１４５を介してコンピュータ１４０と接続されている。

【０２０４】コンピュータ１４０は、ハードディスク１４１と、コントローラ１４２と、外部インタフェース１４３とを備える。そして、ハードディスク１４１はバスＢＳ５を介してコントローラ１４２と接続され、コントローラ１４２はライセンス保護モジュール１４３を含む。

【０２０５】ハードディスク１４１は、インターネット配信によってコンピュータ１４０に配信された暗号化コンテンツデータ｛Ｄａｔａ｝ＫｃをバスＢＳ５を介して記憶する。コントローラ１４２は、携帯電話機１００のユーザから通信ケーブル１４５および外部インタフェース１４３を介して暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃの送信要求があると、ハードディスク１４１から暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを読出し、外部インタフェース１４３を介して外部へ出力する。

【０２０６】外部インタフェース１４３は、携帯電話機１００から通信ケーブル１４５を介してコンピュータ１４０に入力された信号をコントローラ１４２に入力するとともに、コントローラ１４２からの信号を外部へ出力する。

【０２０７】ライセンス保護モジュール１４４は、図５に示すデータ処理部３１０と同じ構成を有し、携帯電話機１００に装着されたメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを送信するために、上述したように携帯電話機１００およびメモリカード１１０と公開暗号鍵、セッションキー等のやり取りを行ないながら、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを保護してメモリカード１１０へ送信するものである。

【０２０８】インターネット配信によって配信サーバからコンピュータ１４０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃが配信され、コンピュータ１４０のハードディスク１４１にバスＢＳ５を介して暗号化コンテンツデータが記憶されている。

【０２０９】携帯電話機１００のユーザがキー操作部１１０８から送信要求を入力すると、通信ケーブル１４５および外部インタフェース１４３を介して送信要求がコントローラ１４２に入力される。コントローラ１４２は、送信要求を受付けると、要求された暗号化コンテンツデータ｛Ｄａｔａ｝ＫｃをバスＢＳ５を介してハードディスク１４１から読出し、ライセンス保護モジュール１４４に入力する。

【０２１０】ライセンス保護モジュール１４４は、上述したようにメモリカード１１０と通信ケーブル１４５を介して公開暗号鍵、セッションキー等のやり取りを行ない、暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃをメモリカード１１０へ送信する。

【０２１１】送信後、携帯電話機１００のユーザは、上述したのと同じ方法によって暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃのライセンス（コンテンツＩＤ、ライセンス鍵Ｋｃ、再生回数制限ＡＣ１、および再生期限ＡＣ２）を配信サーバ３０から配信してもらい、暗号化コ

ンテンツデータ｛Ｄａｔａ｝Ｋｃを再生する。

【０２１２】ＣＤを用いた場合、音楽ＣＤから取得して生成した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、一旦、ハードディスク１４１に記録してからメモリカード１１０へ送信しても良いし、ハードディスク１４１に送信せずに、直接、メモリカード１１０へ送信しても良い。

【０２１３】暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃは、図１９に示すようにメモリカード１１０を、直接、コンピュータ１４０に装着してメモリカード１１０に暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを記録しても良い。この場合、コンピュータ１４０のコントローラ１４２は、ライセンス保護モジュール１４４によって、直接、メモリカード１１０に暗号化コンテンツデータを記録する。

【０２１４】図１９においても、コンピュータ１４０は、図１８に示す場合と同じ方法により暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを取得する。

【０２１５】携帯電話機１００が、新たに受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃに対応するライセンス鍵を含むライセンスの配信要求を配信サーバ３０へ行なう場合のフローチャート、および新たに受信した暗号化コンテンツデータ｛Ｄａｔａ｝Ｋｃを再生するフローチャートは、図９～図１２、および図１５，１６に示すフローチャートと同じである。

【０２１６】再生回数期限ＡＣ１および再生期限ＡＣ２を、それぞれ、再生回数制限と再生期限として説明したが、再生回数期限ＡＣ１は記録装置でのライセンスの扱いに制限を加える制御情報であればよく、また、再生回数はデータ再生端末における再生に対して制限を加えるものであれば何れの制限を行ってもかまわない。

【０２１７】また、携帯電話機１００を暗号化コンテンツデータまたはライセンスの配信を受けるデータ端末装置として説明したが、特に通話機能等は必要なく、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【０２１８】さらには、携帯電話機１００はコンテンツデータ（音楽データ）を再生する機能を備えているが、必ずしもデータ再生機能を必要とせず、ただ、暗号化コンテンツデータまたはライセンスの受信を行えるデータ通信機能を備え、受信したデータを記録できればいかなるデータ端末装置であってもよい。

【０２１９】またさらに、着脱可能な記録装置であるメモリカードに暗号化コンテンツデータまたはライセンスを記録するように説明したが、メモリカードに限定するものではない。そして、実施の形態においては、着脱可能な記録装置である必要もない。

【０２２０】本発明の実施の形態によれば、携帯電話機は、ユーザから暗号化コンテンツデータの配信要求が入力されると、装着されたメモリカードの記録状況を検索し、その記録状況に応じて必要な暗号化コンテンツデータ、およびライセンス鍵等だけを配信サーバから受信するので、暗号化コンテンツデータ、およびライセンス鍵等が重複してメモリカードに記録されることがない。また、ライセンスを重複して受信することによる無駄な料金を配信サーバへ支払うことを防止できる。さらに、暗号化コンテンツデータを重複して受信することによって無駄な時間が発生するのを防止できる。

【０２２１】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。。

【図５】　ライセンスサーバの構成を示す概略ブロック図である。

【図６】　携帯電話機の構成を示すブロック図である。

【図７】　メモリカードの構成を示すブロック図である。

【図８】　メモリカードの記録状態を説明するための概念図である。

【図９】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信動作を説明するための第３のフローチャートである。

【図１２】　図１に示すデータ配信システムにおける配信動作を説明するための第４のフローチャートである。

【図１３】　配信サーバから携帯電話機に送信されたコンテンツメニューを携帯電話機の表示部に表示した状態を示す図である。

【図１４】　メモリカードのメモリにおけるデータフォーマットである。

【図１５】　携帯電話機における再生動作を説明するための第１のフローチャートである。

【図１６】　携帯電話機における再生動作を説明するための第２のフローチャートである。

【図１７】　メモリカードの記録状況に応じた暗号化コンテンツデータおよびライセンスの配信例を説明する図

である。

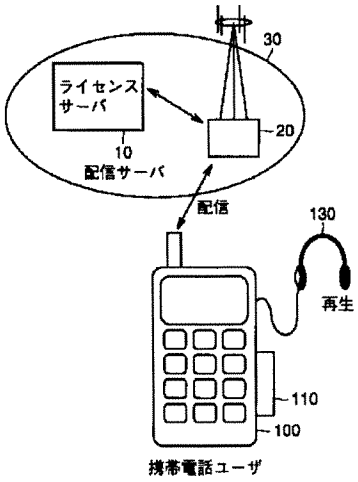
【図１８】　コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための概略図である。

【図１９】　コンピュータを用いた暗号化コンテンツデータの配信を概念的に説明するための他の概略図である。

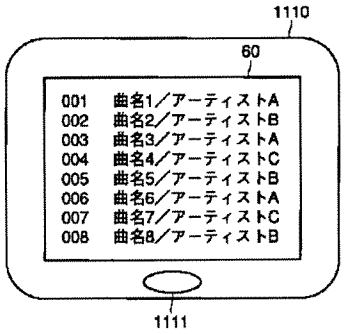
【符号の説明】

１０　ライセンスサーバ、２０　配信キャリア、３０　配信サーバ、６０　コンテンツメニュー、１００　携帯電話機、１１０　メモリカード、１３０　ヘッドホーン、１４０　コンピュータ、１４１　ハードディスク、１４２，１１０６，１４２０　コントローラ、１４３　外部インタフェース、１４４　ライセンス保　護モジュール、１４５　通信ケーブル、３０２　課金データベース、３０４情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１２０６，１２１２，１２１４，１４０４，１４０８，１４１２，１４２２復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１２１０，１４１８　セッションキー発生部、３１８，３２６，３２８，１２０８，１４０６，１４１０　暗号処理部、３５０　通信装置、１１０２　アンテナ、１１０４送受信部、１１０８　キー操作部、１１１０　ディスプレイ、１１１１　移行部、１１１２　音声再生部、１１１３，１２１８　ＤＡ変換器、１１１４，１２０１，１２２０，１２２４　端子、１１１５　マイク、１１１６　ＡＤ変換器、１１１７　音声符号化部、１２００　メモリインタフェース、１２０２，１４００　認証データ保持部、１２０４　Ｋｐ１保持部、１２１６　音楽再生部、１２２２　スイッチ、１４０２　Ｋｍｃ１保持部、１４１４　ＫＰｍａ保持部、１４１５　メモリ、１４１５Ａ　ＣＲＬ領域、１４１５Ｂ　データ領域、１４１６ＫＰｍ１保持部、１４２１　Ｋｍ１保持部、１４２３　インタフェース、１４２４　Ｈｅａｄｅｒ、１４４０　ライセンス情報保持部、１４４２，１４４４，１４４６　切換スイッチ。

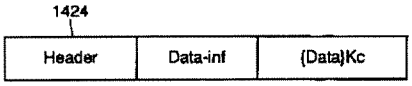
【図１】



【図１３】



【図１４】



【図４】

名称	属性	保持／発生箇所	機能・特徴
Ks1	共通鍵	配信サーバ	配信セッション毎に発生
Ks2		メモリカード	配信／再生セッション毎に発生
Ks3		携帯電話機	再生セッション毎に発生
Km	秘密復号鍵	メモリカード	メモリカードごとに固有の復号鍵 KPmで暗号化されたデータはKmで復号可能
KPm	公開暗号鍵 （非対称鍵）	メモリカード	メモリカードごとに固有の暗号鍵
KPma	公開認証鍵	配信サーバ	配信システム全体で共通。

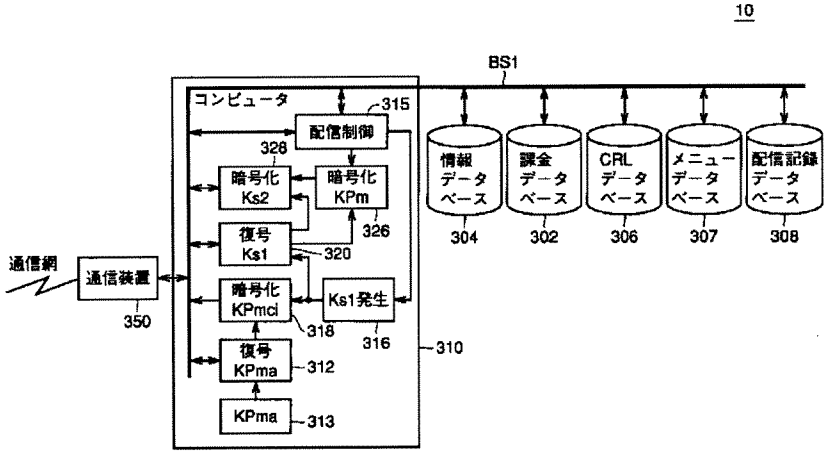
【図２】

名称	属性	保持／発生箇所	機能・特徴
Data	コンテンツデータ	配信サーバ	例：音楽データ、アップデートプログラム
Kc	ライセンス鍵		暗号化コンテンツデータの復号鍵
{Data}Kc	暗号化コンテンツデータ		共通鍵Kcで復号可能な暗号化が施されたコンテンツデータこの形式で配信サーバより配布。
Data-inf	付加情報		例：コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報
コンテンツID	コンテンツに関する情報		コンテンツデータDataを識別するコード
ライセンスID	ライセンスに関する情報		ライセンスの発行を特定できる管理コード（コンテンツIDを含めて識別することも可）
トランザクションID	ライセンス固有		配信を特定するための管理コード
AC	ライセンス購入条件		利用者側から指定(例：ライセンス数,機能限定等)
AC1	アクセス制限情報		メモリのアクセスに対する制限(例：再生可能回数)
AC2	再生回路制御情報		コンテンツ再生回路(携帯電話機)における制御情報（例：再生可否）

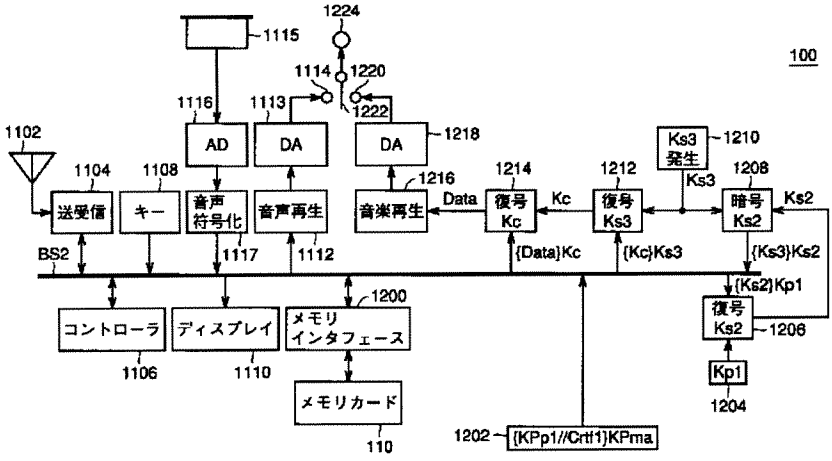
【図３】

名称	属性	保持／発生箇所	機能・特徴
CRL	禁止クラスリスト関連情報	配信サーバ メモリカード	禁止クラスリストの対象クラスデータ
CRL_dat		配信サーバ	禁止クラスリストのバージョン更新のための情報
CRL_ver		メモリカード	禁止クラスリストのバージョン情報
KPpn	公開暗号鍵（非対称鍵）	携帯電話機	Kpnにて復号可能。{KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機の種類nごとに異なる。
KPmci	公開暗号鍵（非対称鍵）	メモリカード	Kmciにて復号可能。{KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードの種類iごとに異なる。
Kpn	秘密復号鍵	携帯電話機	コンテンツ再生回路(携帯電話機)固有の復号鍵 ＊携帯電話機の種類nごとに異なる。
Kmci	秘密復号鍵	メモリカード	メモリカード固有の復号鍵 ＊メモリカードの種類iごとに異なる。
Crtfn	クラス証明書	携帯電話機	コンテンツ再生回路のクラス証明書。認証機能を有する。{KPpn//Crtfn}KPmaの形式で出荷時に記録 ＊携帯電話機のクラスnごとに異なる。
Cmci		メモリカード	メモリカードのクラス証明書。認証機能を有する。{KPmci//Cmci}KPmaの形式で出荷時に記録 ＊メモリカードのクラスiごとに異なる。

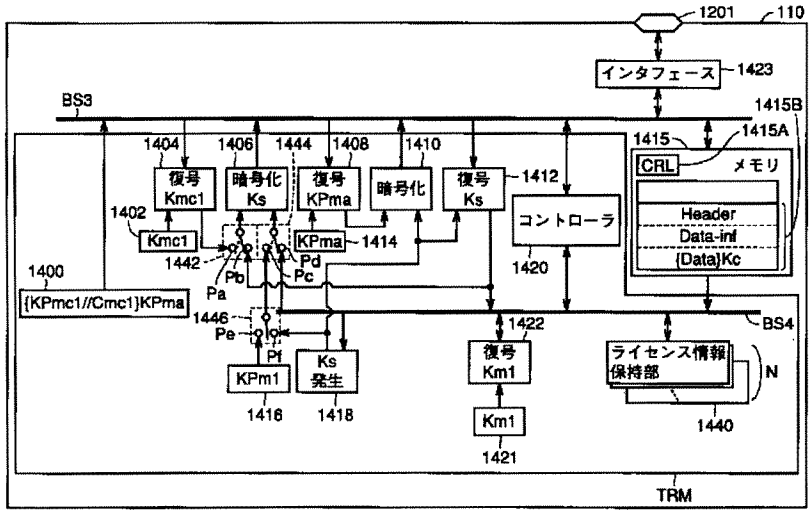
【図５】



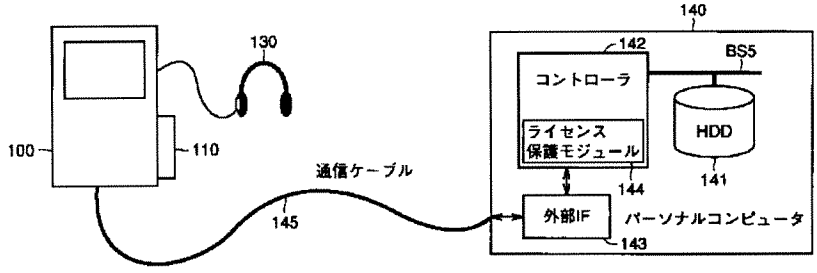
【図６】


100
1224
1115
1114
1220
1222
1116
1113
1102
AD
DA
DA
1218
Ks3
発生
1210
1104
1108
1216
1214
1212
1208
送受信
キー
音声
符号化
音声再生
音楽再生
Data
復号
Kc
Kc
復号
Ks3
暗号
Ks2
Ks2
BS2
1117
1112
{Data}Kc
{Kc}Ks3
{Ks3}Ks2
{Ks2}Kp1
1200
復号
Ks2
1206
コントローラ
ディスプレイ
メモリ
インタフェース
1106
1110
Kp1
1204
メモリカード
110
1202
{KPp1//Crtf1}KPma

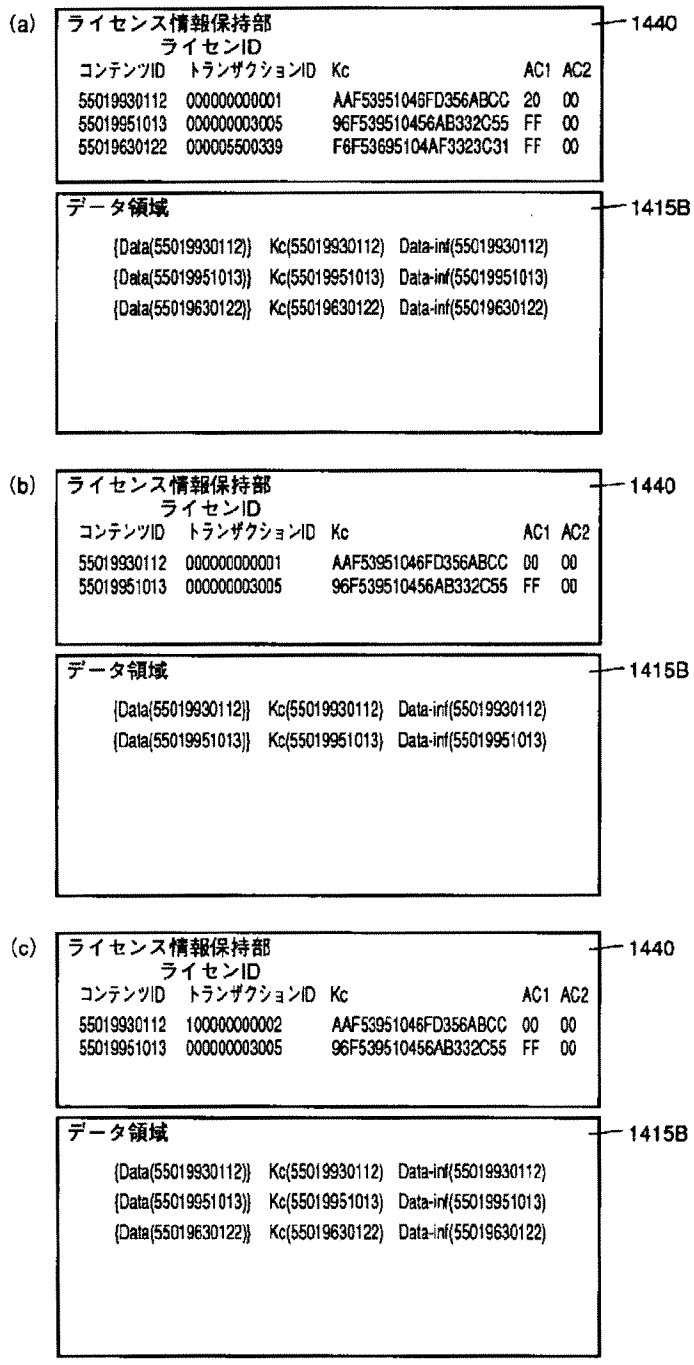
【図７】


1201
110
インタフェース
1423
BS3
1415B
1404
1406
1444
1408
1410
1415
1415A
CRL
メモリ
復号
Kmc1
暗号化
Ks
復号
KPma
暗号化
復号
Ks
1412
1402
Header
Data-inf
{Data}Kc
Kmc1
KPma
1414
1442
Pb
Pd
Pa
Pc
1400
{KPmc1//Cmc1}KPma
コントローラ
1420
1446
Pe
BS4
1422
Pf
復号
Km1
ライセンス情報
保持部
N
KPm1
Ks
発生
1416
1418
Km1
1421
1440
TRM

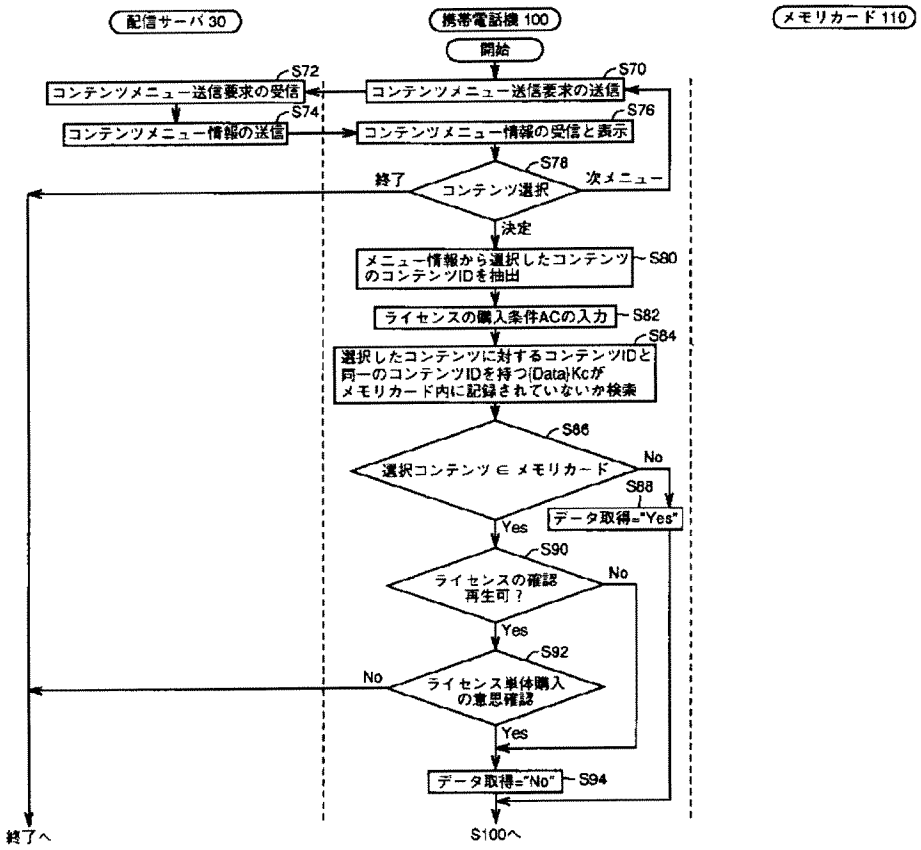
【図１８】


140
130
142
BS5
コントローラ
100
110
ライセンス
保護モジュール
HDD
通信ケーブル
144
141
外部IF
パーソナルコンピュータ
145
143

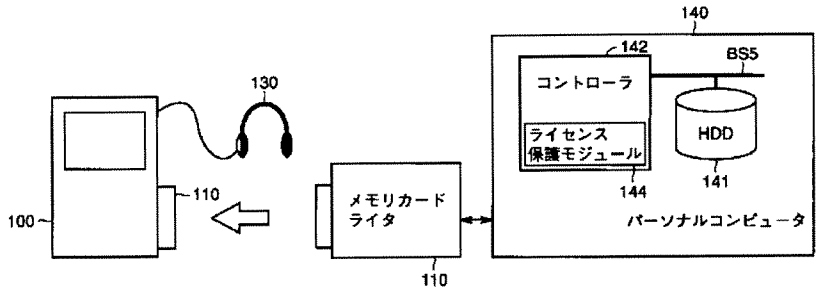
【図８】


(a)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 20 00
55019951013 000000003005 96F539510456AB332C55 FF 00
55019630122 000005500339 F6F53695104AF3323C31 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
(b)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 000000000001 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F539510456AB332C55 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
1415B
(c)
ライセンス情報保持部
ライセンID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 100000000002 AAF53951046FD356ABCC 00 00
55019951013 000000003005 96F539510456AB332C55 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B

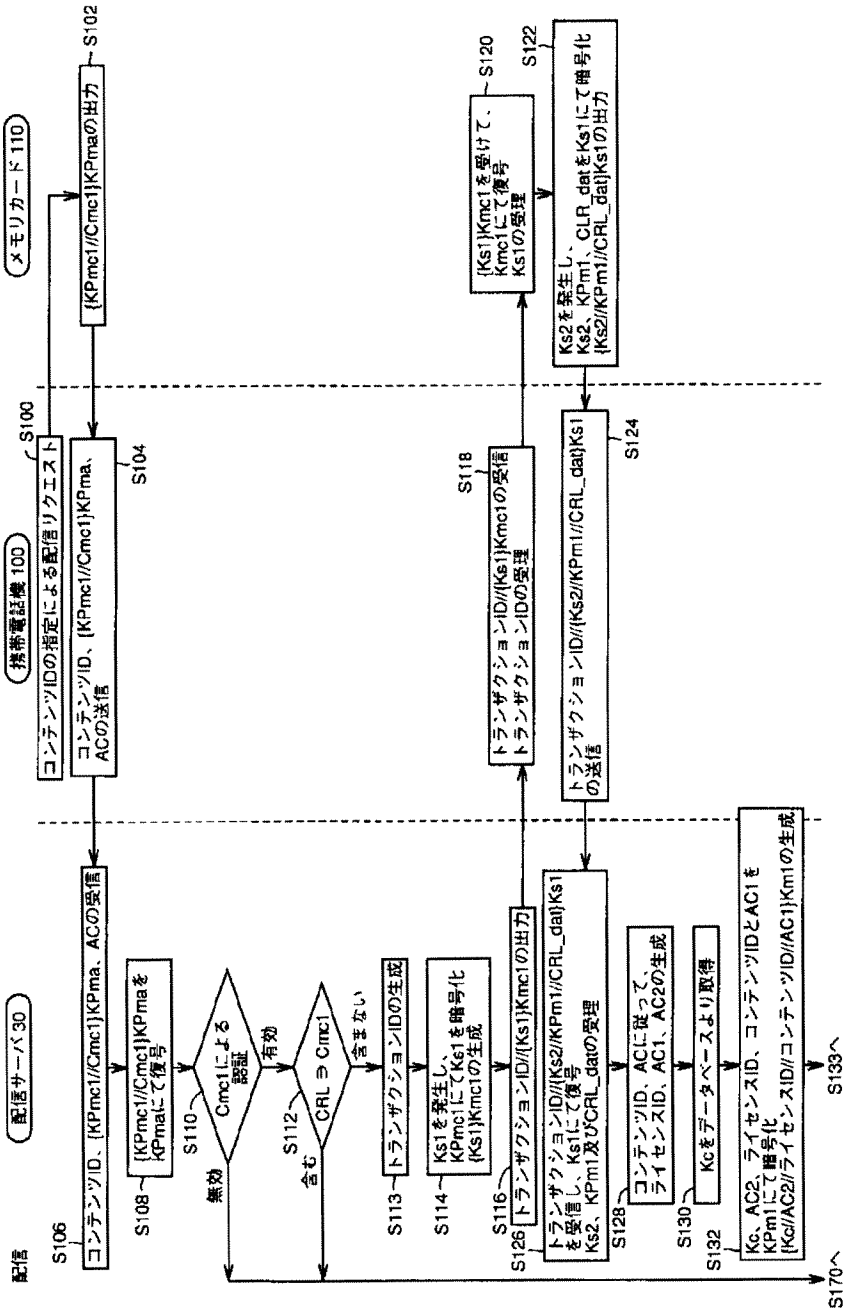
【図９】


配信サーバ30
携帯電話機100
メモリカード110
開始
S70
コンテンツメニュー送信要求の送信
S72
コンテンツメニュー送信要求の受信
S74
コンテンツメニュー情報の送信
S76
コンテンツメニュー情報の受信と表示
S78
コンテンツ選択
終了
次メニュー
決定
メニュー情報から選択したコンテンツのコンテンツIDを抽出
S80
ライセンスの購入条件ACの入力
S82
S84
選択したコンテンツに対するコンテンツIDと同一のコンテンツIDを持つ{Data}Kcがメモリカード内に記録されていないか検索
S86
選択コンテンツ∈メモリカード
No
S88
データ取得="Yes"
Yes
S90
ライセンスの確認
再生可？
No
Yes
S92
No
ライセンス単体購入の意思確認
Yes
データ取得="No"
S94
終了へ
S100へ

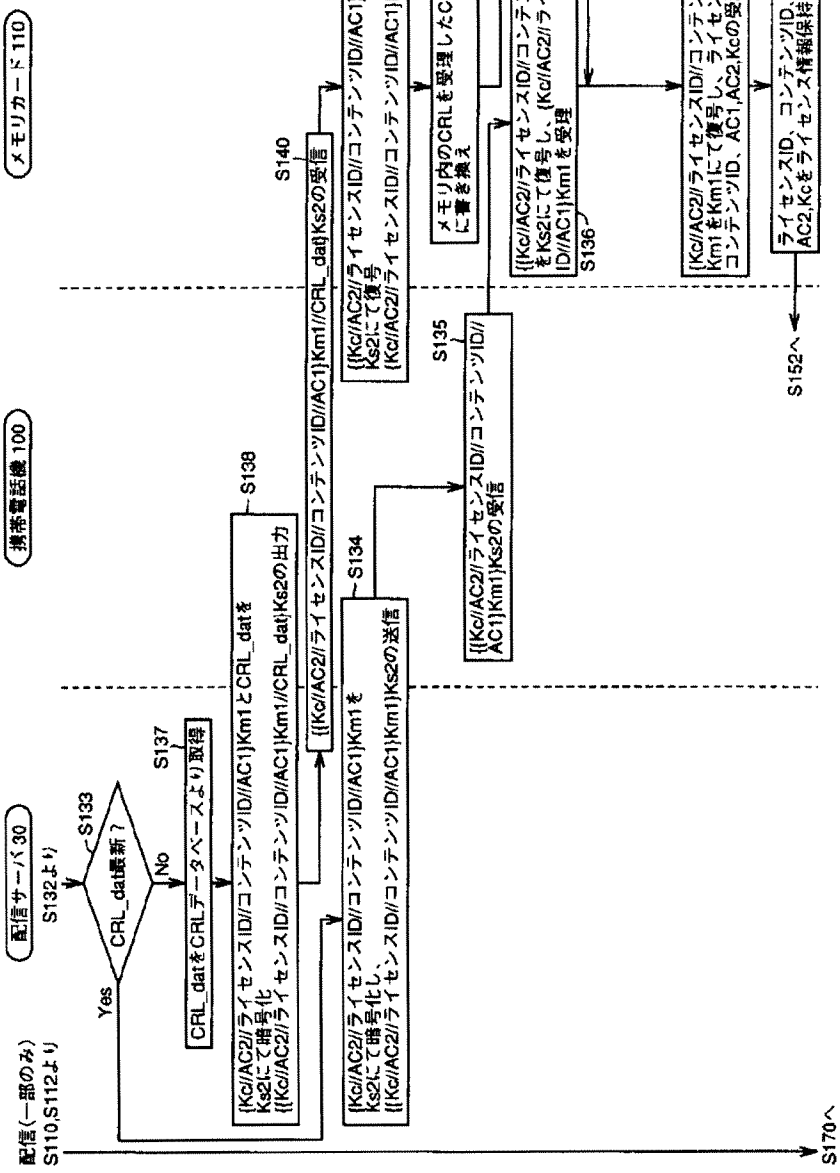
【図１９】


140
142
BS5
コントローラ
ライセンス保護モジュール
HDD
144
141
パーソナルコンピュータ
130
110
100
メモリカードライタ
110

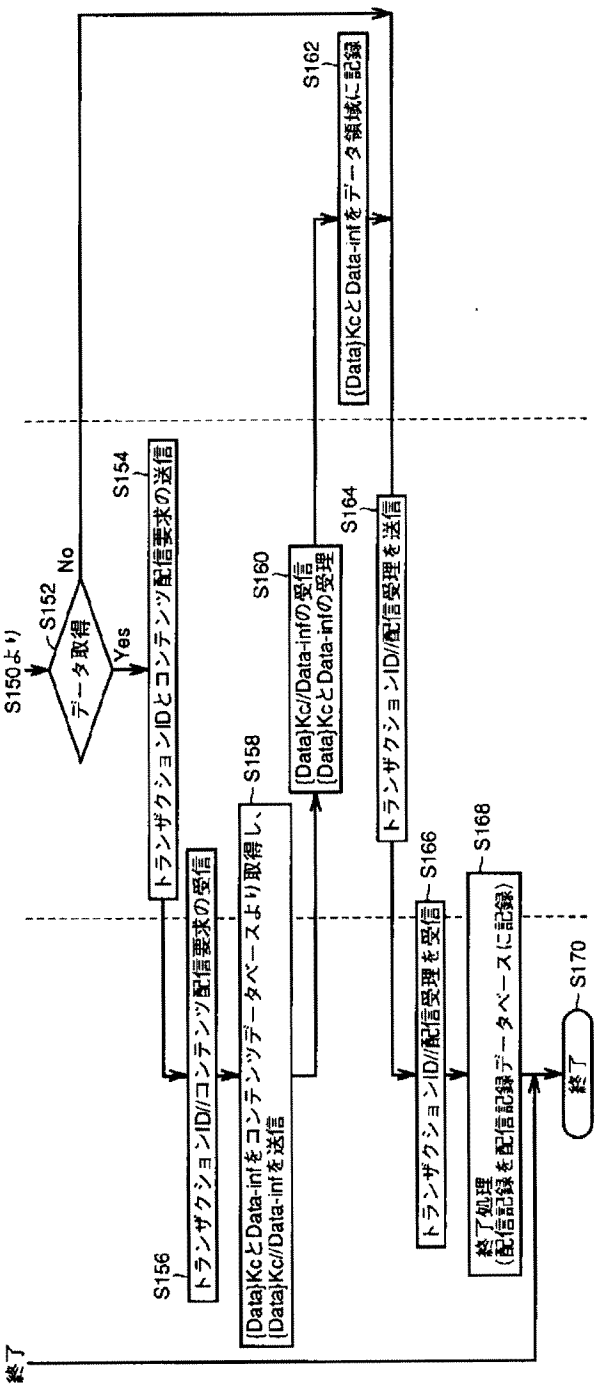
【図１０】


メモリカード 110
携帯電話機 100
配信サーバ 30
配信
コンテンツIDの指定による配信リクエスト
S100
コンテンツID、{KPmc1//Cmc1}KPmaの出力
S102
コンテンツID、{KPmc1//Cmc1}KPma、ACの送信
S104
S106
コンテンツID、{KPmc1//Cmc1}KPma、ACの受信
S108
{KPmc1//Cmc1}KPmaをKPmaにて復号
S110
Cmc1による認証
無効
有効
S112
CRL ∋ Cmc1
含む
含まない
S113
トランザクションIDの生成
S114
Ks1を発生し、KPmc1にてKs1を暗号化{Ks1}Kmc1の生成
S116
トランザクションID//{Ks1}Kmc1の出力
S118
トランザクションID//{Ks1}Kmc1の受理
S120
{Ks1}Kmc1を受けて、Kmc1にて復号Ks1の受理
S122
Ks2を発生し、Ks2、KPm1、CLR_datをKs1にて暗号化{Ks2//KPm1//CRL_dat}Ks1の出力
S124
トランザクションID//{Ks2//KPm1//CRL_dat}Ks1の送信
S126
トランザクションID//{Ks2//KPm1//CRL_dat}Ks1を受信し、Ks1にて復号Ks2、KPm1及びCRL_datの受理
S128
コンテンツID、ACに従って、ライセンスID、AC1、AC2の生成
S130
Kcをデータベースより取得
S132
Kc、AC2、ライセンスID、コンテンツIDとAC1をKPm1にて暗号化{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1の生成
S133へ
S170へ

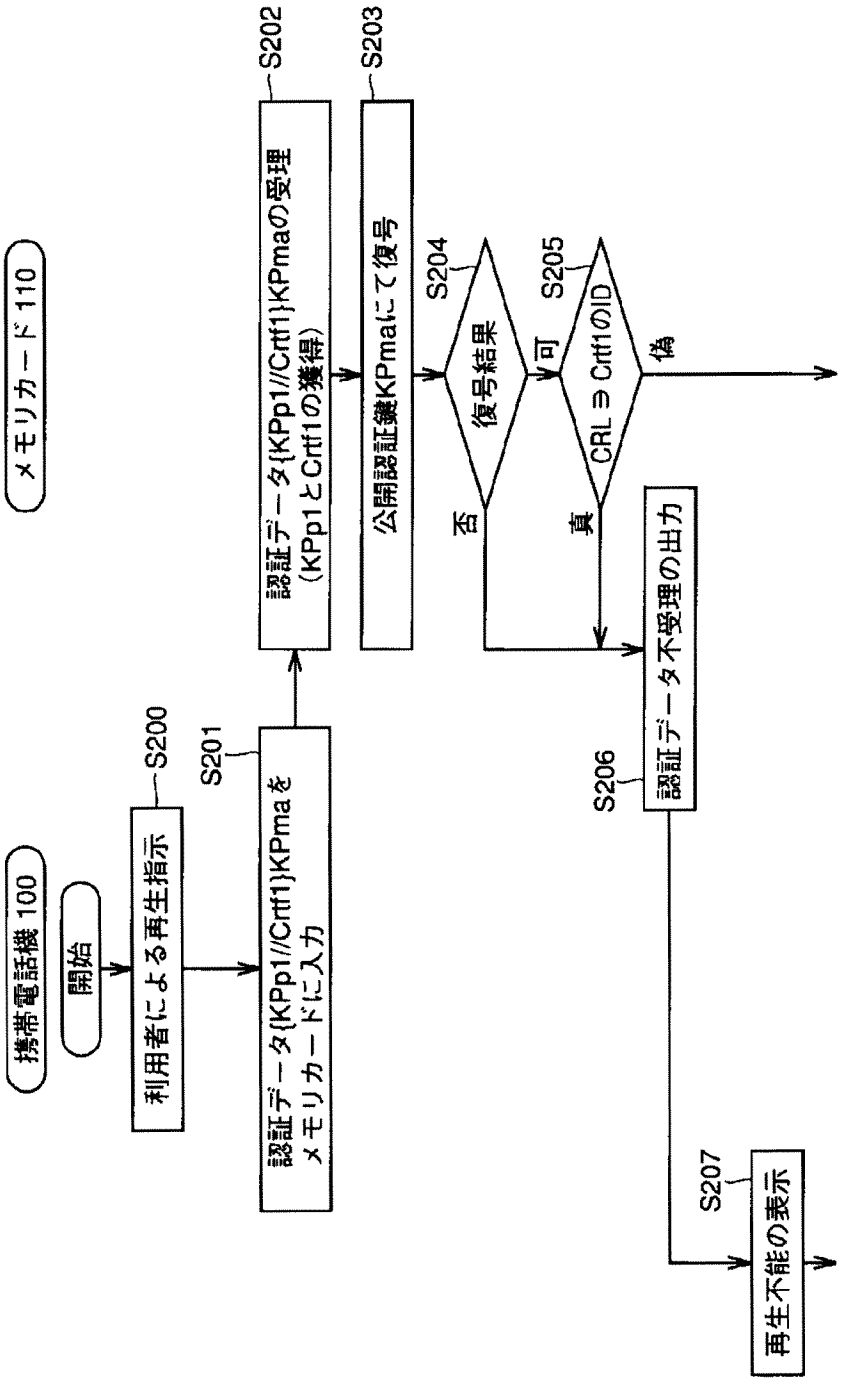
【図１１】


メモリカード 110
携帯電話機 100
配信サーバ 30
配信(一部のみ)
S110,S112より
S132より
S133
CRL_datを最新？
Yes
No
S137
CRL_datをCRLデータベースより取得
S138
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datを
Ks2にて暗号化
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の出力
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の受信
S140
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1を
Ks2にて暗号化し、
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2の送信
S134
{{Kc//AC2//ライセンスID//
AC1}Km1}Ks2の受信
S135
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1//CRL_dat}Ks2を
Ks2にて復号
{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1とCRL_datの受理
S142
メモリ内のCRLを受理したCRL_dat
に書き換え
S144
{{Kc//AC2//ライセンスID//コンテンツID//AC1}Km1}Ks2
をKs2にて復号し、{Kc//AC2//ライセンスID//コンテンツ
ID//AC1}Km1を受理
S136
{Kc//AC2//ライセンスID//コンテンツID//AC1}
Km1をKm1にて復号し、ライセンスID、
コンテンツID、AC1,AC2,Kcの受理
S148
ライセンスID、コンテンツID、AC1,
AC2,KcをライセンスI情報保持部に記録
S150
S152へ
S170へ

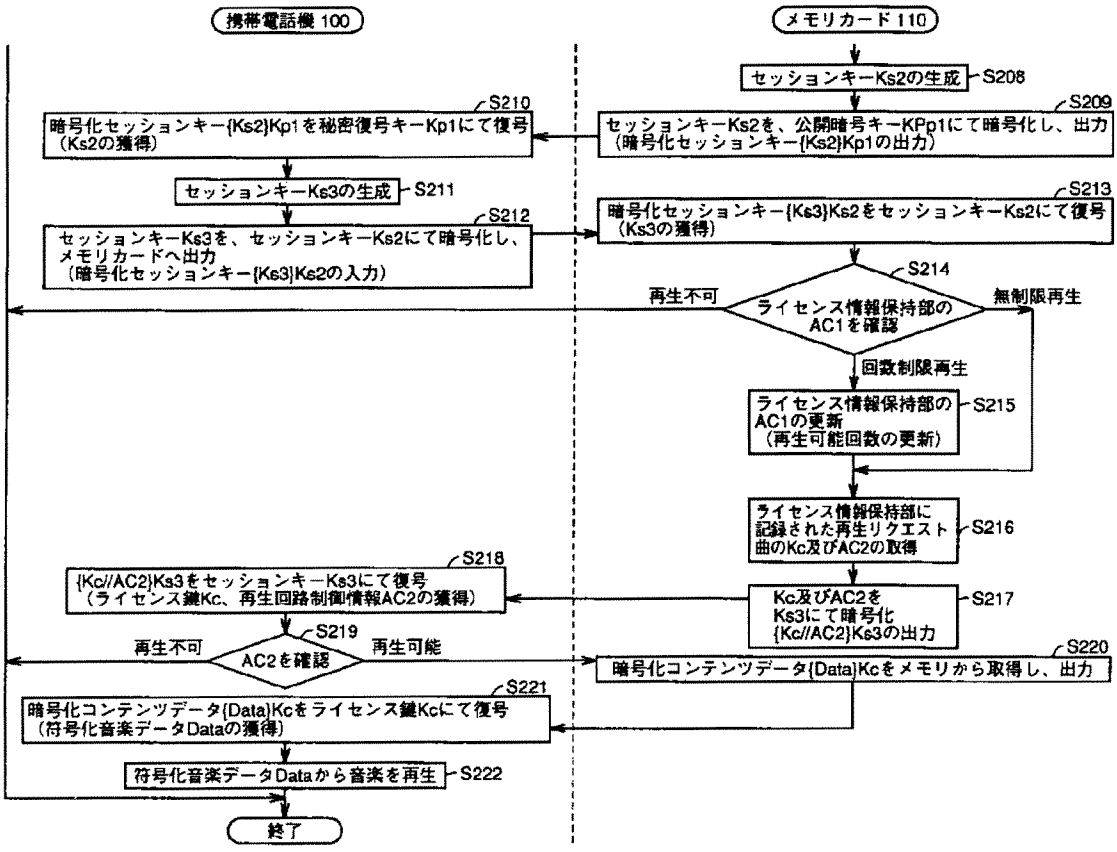
【図１２】


配信サーバ30
携帯電話機100
メモリカード110
S150より
S152
データ取得
No
Yes
S154
トランザクションIDとコンテンツ配信要求の送信
S156
トランザクションID//コンテンツ配信要求の受信
S158
{Data}Kcと{Data}Kc//Data-infを送信
{Data}Kc//Data-infをコンテンツデータベースより取得し、
S160
{Data}Kc//Data-infの受信
{Data}KcとData-infの受理
S162
{Data}KcとData-infをデータ領域に記録
S164
トランザクションID//配信受理を送信
S166
トランザクションID//配信受理を受信
S168
終了処理
(配信記録を配信記録データベースに記録)
S170
終了
終了

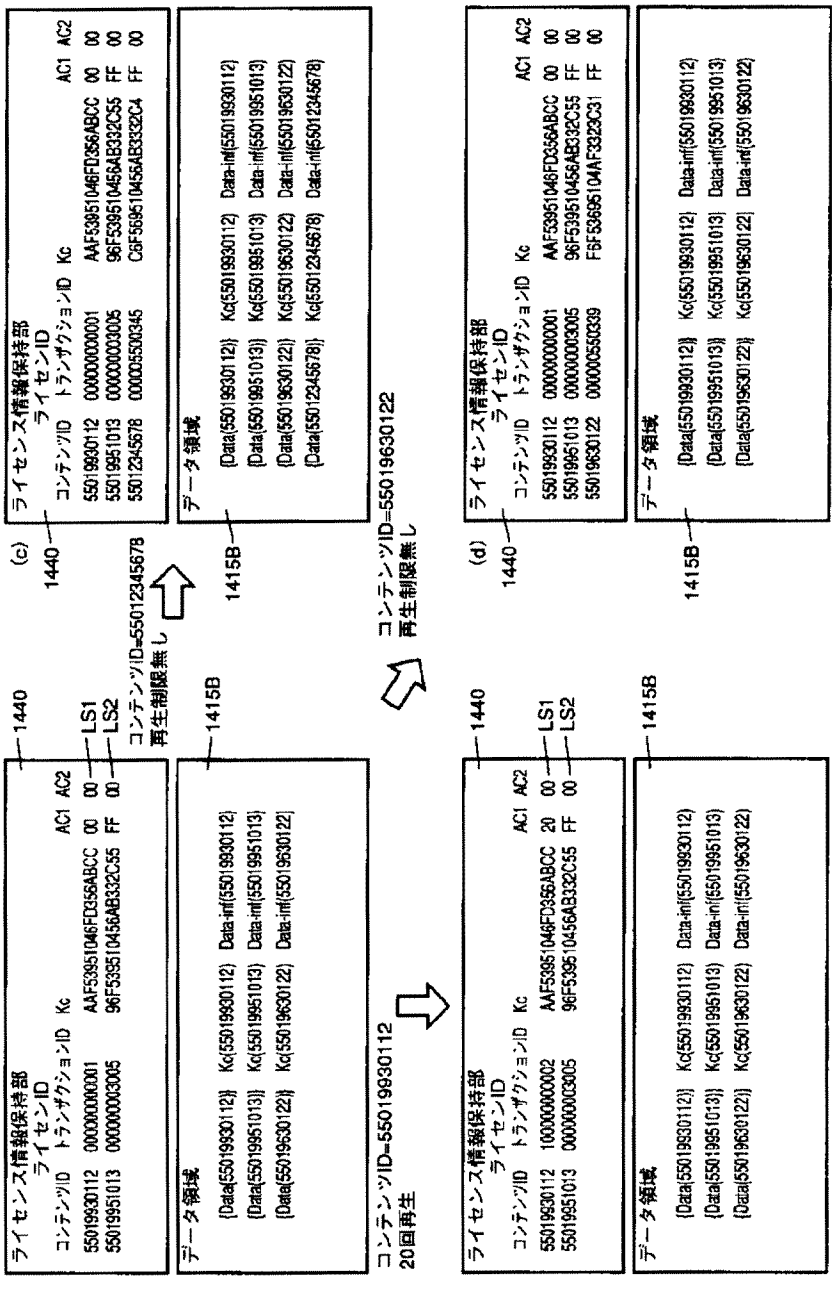
【図１５】


携帯電話機 100
メモリカード 110
開始
利用者による再生指示
S200
認証データ{KPp1//Crtf1}KPmaをメモリカードに入力
S201
認証データ{KPp1//Crtf1}KPmaの受理(KPp1とCrtf1の獲得)
S202
公開認証鍵KPmaにて復号
S203
復号結果
S204
否
可
CRL ∋ Crtf1のID
S205
真
偽
認証データ不受理の出力
S206
再生不能の表示
S207

【図１６】


携帯電話機 100
メモリカード 110
セッションキーKs2の生成
S208
S209
セッションキーKs2を、公開暗号キーKPp1にて暗号化し、出力
（暗号化セッションキー{Ks2}Kp1の出力）
S210
暗号化セッションキー{Ks2}Kp1を秘密復号キーKp1にて復号
（Ks2の獲得）
セッションキーKs3の生成
S211
S212
セッションキーKs3を、セッションキーKs2にて暗号化し、
メモリカードへ出力
（暗号化セッションキー{Ks3}Ks2の入力）
S213
暗号化セッションキー{Ks3}Ks2をセッションキーKs2にて復号
（Ks3の獲得）
S214
再生不可
ライセンス情報保持部の
AC1を確認
無制限再生
回数制限再生
ライセンス情報保持部の
AC1の更新
（再生可能回数の更新）
S215
ライセンス情報保持部に
記録された再生リクエスト
曲のKc及びAC2の取得
S216
S218
{Kc//AC2}Ks3をセッションキーKs3にて復号
（ライセンス鍵Kc、再生回路制御情報AC2の獲得）
Kc及びAC2を
Ks3にて暗号化
{Kc//AC2}Ks3の出力
S217
S219
再生不可
AC2を確認
再生可能
S220
暗号化コンテンツデータ{Data}Kcをメモリから取得し、出力
S221
暗号化コンテンツデータ{Data}Kcをライセンス鍵Kcにて復号
（符号化音楽データDataの獲得）
符号化音楽データDataから音楽を再生
S222
終了

【図１７】


(a)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 0000000000001 AAF539510461FD356ABCC 00 00
55019951013 0000000003005 96F53951045 6AB332C55 FF 00
1440
LS1
LS2
コンテンツID=55012345678
再生制限無し
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
コンテンツID=55019930112
20回再生
(b)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 1000000000002 AAF539510461FD356ABCC 20 00
55019951013 0000000003005 96F53951045 6AB332C55 FF 00
1440
LS1
LS2
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B
コンテンツID=55019630122
再生制限無し
(c)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 0000000000001 AAF539510461FD356ABCC 00 00
55019951013 0000000003005 96F53951045 6AB332C55 FF 00
55012345678 0000005500345 C6F56961045 6AB332C4 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
{Data(55012345678)} Kc(55012345678) Data-inf(55012345678)
1415B
(d)
ライセンス情報保持部
ライセンスID
コンテンツID トランザクションID Kc AC1 AC2
55019930112 0000000000001 AAF539510461FD356ABCC 00 00
55019951013 0000000003005 96F53951045 6AB332C55 FF 00
55019630122 0000005500339 F6F53695104AF3323C31 FF 00
1440
データ領域
{Data(55019930112)} Kc(55019930112) Data-inf(55019930112)
{Data(55019951013)} Kc(55019951013) Data-inf(55019951013)
{Data(55019630122)} Kc(55019630122) Data-inf(55019630122)
1415B